

# A NON-COMMUTATIVE REAL NULLSTELLENSATZ CORRESPONDS TO A NON-COMMUTATIVE REAL IDEAL; ALGORITHMS

JAKOB CIMPRIČ<sup>1</sup>, J. WILLIAM HELTON<sup>2</sup>, SCOTT MCCULLOUGH<sup>3</sup>,  
AND CHRISTOPHER NELSON<sup>2†</sup>

ABSTRACT. This article extends the classical Real Nullstellensatz of Dubois and Risler to left ideals in free  $*$ -algebras  $\mathbb{R}\langle x, x^* \rangle$  with  $x = (x_1, \dots, x_n)$ .

First we introduce notions of the (noncommutative) zero set of a left ideal and of a real left ideal. We prove that every element from  $\mathbb{R}\langle x, x^* \rangle$  whose zero set contains the intersection of zero sets of elements from a finite subset  $S$  of  $\mathbb{R}\langle x, x^* \rangle$  belongs to the smallest real left ideal containing  $S$ .

Next we give an implementable algorithm which for every finite  $S \subset \mathbb{R}\langle x, x^* \rangle$  computes the smallest real left ideal containing  $S$  and prove that the algorithm succeeds in a finite number of steps.

Our definitions and some of our results also work for other  $*$ -algebras. As an example we treat real left ideals in  $M_n(\mathbb{R}[x_1])$ .

## 1. INTRODUCTION

This article establishes analogs, in the setting of (some)  $*$ -algebras, of the classical real Nullstellensatz of Dubois and Risler. Accordingly, to state results, it is first necessary to discuss both noncommutative zero sets and real ideals and radicals. These topics are treated below in Subsections 1.1 and 1.2 respectively. The introduction concludes with a brief discussion of the main results in Subsection 1.3.

---

1991 *Mathematics Subject Classification.* 16W10, 16S10, 16Z05, 14P99, 14A22, 47Lxx, 13J30.

*Key words and phrases.* noncommutative real algebraic geometry, algebras with involution, free algebras, matrix polynomials, symbolic computation.

<sup>1</sup>Research supported by the grant P1-0222 from the Slovenian Research Agency ARRS.

<sup>2</sup>Research supported by NSF grants DMS-0700758, DMS-0757212, and the Ford Motor Co.

<sup>3</sup>Research supported by the NSF grant DMS-0758306.

<sup>†</sup>Much of the material in this paper is part of the Ph.D. thesis of Christopher Nelson at UCSD.

Our approach to Noncommutative Real Algebraic Geometry is motivated by [4]; for alternative approaches see [12] and [7].

**1.1. Zero Sets in  $*$ -Algebras.** Let  $F$  be either  $\mathbb{R}$  or  $\mathbb{C}$  with complex conjugation as involution. Let  $\mathcal{A}$  be a unital associative  $F$ -algebra with involution  $*$ , or  $*$ -algebra for short. Let  $V$  be a pre-Hilbert space, i.e. an  $F$ -vector space with an inner product. A mapping  $\pi$  of  $\mathcal{A}$  into the set of  $F$ -linear operators defined on  $V$  is said to be a (unital)  $*$ -representation of  $\mathcal{A}$  on  $V$  if  $\pi(1) = 1$  and it satisfies the familiar axioms:

$$\begin{aligned}\pi(\alpha_1 a_1 + \alpha_2 a_2)v &= \alpha_1 \pi(a_1)v + \alpha_2 \pi(a_2)v \\ \pi(a_1 a_2)v &= \pi(a_1)\pi(a_2)v \\ \langle \pi(a)v_1, v_2 \rangle &= \langle v_1, \pi(a^*)v_2 \rangle\end{aligned}$$

for every  $a, a_1, a_2 \in \mathcal{A}$ ,  $\alpha_1, \alpha_2 \in F$  and  $v, v_1, v_2 \in V$ .

Let  $\mathcal{R}$  be the class of all  $*$ -representations of the  $*$ -algebra  $\mathcal{A}$ . Usually, we are only interested in some subclass of “well-behaved”  $*$ -representations, such as the subclass  $\Pi$  of all finite-dimensional  $*$ -representations. In the following let  $\mathcal{C}$  be a fixed subclass of  $\mathcal{R}$ .

A  $\mathcal{C}$ -point of  $\mathcal{A}$  is an ordered pair  $(\pi, v)$  such that  $\pi \in \mathcal{C}$  and  $v \in V_\pi$ . Write  $\text{pt}_{\mathcal{C}}(\mathcal{A})$  for the set of all  $\mathcal{C}$ -points of the  $*$ -algebra  $\mathcal{A}$ . For every subset  $S$  of  $\mathcal{A}$  write

$$V_{\mathcal{C}}(S) := \{(\pi, v) \in \text{pt}_{\mathcal{C}}(\mathcal{A}) \mid \pi(s)v = 0 \text{ for every } s \in S\}.$$

Clearly,  $V_{\mathcal{C}}(S) = V_{\mathcal{R}}(S) \cap \text{pt}_{\mathcal{C}}(\mathcal{A})$ . For a subset  $T$  of  $\text{pt}_{\mathcal{R}}(\mathcal{A})$ , let

$$\mathcal{I}(T) := \{a \in \mathcal{A} \mid \pi(a)v = 0 \text{ for every } (\pi, v) \in T\}.$$

Note that  $\mathcal{I}(T)$  is always a left ideal.

Now we give three examples.

**Example 1.1.** Let  $\mathfrak{F} = F\langle x, x^* \rangle$  denote the **free  $*$ -algebra** on  $x = (x_1, \dots, x_g)$ . Given a  $g$ -tuple  $X = (X_1, \dots, X_g)$  of same size square matrices over  $F$ , write  $\pi_X(p) := p(X)$ , where  $p(X)$  is the natural evaluation of  $p$  at  $X$ . It is evident that  $\pi_X$  is a  $*$ -representation of  $\mathfrak{F}$  on the Hilbert space  $F^N$  ( $N$  is the size of  $X$ ) and is thus an element of the class  $\Pi$ . Conversely, every element  $\pi$  of  $\Pi$  is equal to  $\pi_X$  for some  $g$ -tuple  $X$  (namely  $X_j = \pi(x_j)$ ). Therefore, the  $\Pi$ -points of  $\mathfrak{F}$  can be identified with pairs  $(X, v)$  with  $v$  being in  $F^N$ . For  $S \subset \mathfrak{F}$  we have

$$V_{\Pi}(S) = \{(X, v) \mid p(X)v = 0 \text{ for every } p \in S\}.$$

For a subset  $T$  of  $\text{pt}_{\Pi}(\mathfrak{F})$  we have

$$\mathcal{I}(T) = \{p \in \mathfrak{F} \mid p(X)v = 0 \text{ for every } (X, v) \in T\}.$$

As we shall see, in the case of  $\mathfrak{F}$ , for many purposes  $\Pi$  is a well-behaved subclass of  $\mathcal{R}$ .  $\square$

**Example 1.2.** Let  $F[x]$  denote the algebra of all polynomials in variables  $x = (x_1, \dots, x_g)$  with coefficients from  $F \in \{\mathbb{R}, \mathbb{C}\}$ . For every  $n$ , let  $M_n(F[x])$  denote the algebra of  $n \times n$  matrices with entries in  $F[x]$ . The involution  $\bar{\phantom{x}}$  on  $F[x]$  conjugates the coefficients and the involution  $*$  on  $M_n(F[x])$  is the conjugated transpose, i.e.  $[p_{ij}]^* = [\overline{p_{ji}}]$ .

For every point  $a \in \mathbb{R}^g$  its evaluation mapping  $\text{ev}_a: M_n(F[x]) \rightarrow M_n(F)$  defined by  $\text{ev}_a([p_{ij}]) := [p_{ij}(a)]$ , is a  $*$ -representation of  $M_n(F[x])$  on  $F^n$ . (The evaluations in complex points need not be  $*$ -representations.) The class  $\mathcal{E} := \{\text{ev}_a \mid a \in \mathbb{R}^g\}$  is a proper subclass of  $\Pi$ . Note that the  $\mathcal{E}$ -points of  $M_n(F[x])$  can be identified with pairs  $(a, v)$  where  $a \in \mathbb{R}^g$  and  $v \in F^n$ , i.e.  $\text{pt}_{\mathcal{E}}(M_n(F[x])) = \mathbb{R}^g \times F^n$ . For  $S \subset M_n(F[x])$  we have

$$V_{\mathcal{E}}(S) = \{(a, v) \in \mathbb{R}^g \times F^n \mid p(a)v = 0 \text{ for every } p \in S\}.$$

For a subset  $T$  of  $\mathbb{R}^g \times F^n$  we have

$$\mathcal{I}(T) = \{p \in M_n(F[x]) \mid p(a)v = 0 \text{ for every } (a, v) \in T\}.$$

This example also makes sense for  $g = 0$ . In this case  $F[x] = F$ , so that  $M_n(F[x]) = M_n(F)$ . Moreover,  $\mathbb{R}^g = \{0\}$ , so the only element of  $\mathcal{E}$  is  $\text{Id}: M_n(F) \rightarrow M_n(F)$ .  $\square$

**Example 1.3.** The polynomial algebra  $F[y]$ ,  $y = (y_1, \dots, y_g)$ ,  $F \in \{\mathbb{R}, \mathbb{C}\}$ , with involution  $y_i^* = -y_i$  for  $i = 1, \dots, g$  and  $\alpha^* = \bar{\alpha}$  for  $\alpha \in F$  has a natural  $*$ -representation  $\pi_0$  acting on the Schwartz space  $\mathcal{S}(\mathbb{R}^g, F)$  of rapidly decreasing functions. It assigns to each  $y_i$  the partial derivative  $\frac{\partial}{\partial t_i}$  so each  $\pi_0(p)$  is the partial differential operator  $p(D)$ . The set of  $\{\pi_0\}$ -points is  $\text{pt}_{\{\pi_0\}}(\mathcal{W}_g) = \{\pi_0\} \times \mathcal{S}(\mathbb{R}^g, F)$  which can be identified with  $\mathcal{S}(\mathbb{R}^g, F)$ . For every  $S \subseteq \mathbb{R}[y]$  we have

$$V_{\{\pi_0\}}(S) = \{\psi \in \mathcal{S}(\mathbb{R}^g, F) \mid \pi_0(p)\psi = 0 \text{ for every } p \in S\}$$

which is the set of all solutions of the partial differential equations from  $S$ . For a subset  $T$  of  $\mathcal{S}(\mathbb{R}^g, F)$  we have

$$\mathcal{I}(T) = \{p \in \mathbb{R}[y] \mid \pi_0(p)\psi = 0 \text{ for every } \psi \in T\}$$

which is the set of all partial differential equations whose solution sets contain  $T$ . (We will not discuss this example in other sections but see [10] for a Nullstellensatz in the spirit of this paper. The definitions can also be extended to partial differential equations with non-constant coefficients but we are not aware of any results in this direction.)  $\square$

**1.2. Radicals and Noncommutative Real Ideals.** For a left ideal  $I$  of  $\mathcal{A}$  and a class  $\mathcal{C}$  of  $*$ -representations of  $\mathcal{A}$ , we call the radical

$$\sqrt[\mathcal{C}]{I} := \mathcal{I}(V_{\mathcal{C}}(I))$$

the  $\mathcal{C}$ -saturation of  $I$ . Evidently  $\sqrt[\mathcal{C}]{I}$  is a left ideal. We say that  $I$  has the left nullstellensatz property for  $\mathcal{C}$ -points if  $\sqrt[\mathcal{C}]{I} = I$ . Lemma 1.4 lists the basic facts.

**Lemma 1.4.** *Let  $\mathcal{C}$  be a representation class and  $I$  a left ideal of  $\mathcal{A}$ .*

*The radical  $\sqrt[\mathcal{C}]{I}$  is the smallest left ideal which contains  $I$  and has the left nullstellensatz property for  $\mathcal{C}$ -points.*

*For every subset  $S$  of  $\mathcal{A}$ ,  $V_{\mathcal{C}}(S) = V_{\mathcal{C}}(I_S) = V_{\mathcal{C}}(\sqrt[\mathcal{C}]{I_S})$  where  $I_S$  is the left ideal of  $\mathcal{A}$  generated by  $S$ .*

*If  $I \subseteq I'$  then  $\sqrt[\mathcal{C}]{I} \subseteq \sqrt[\mathcal{C}]{I'}$ . If  $\mathcal{C} \subseteq \mathcal{C}'$  then  $\sqrt[\mathcal{C}]{I} \subseteq \sqrt[\mathcal{C}']{I}$ .*

*For every subset  $T$  of  $\text{pt}_{\mathcal{C}}(\mathcal{A})$  we have that  $\sqrt[\mathcal{C}]{\overline{\mathcal{I}(T)}} = \mathcal{I}(T)$ .*

*Proof.* All claims are straightforward consequences of the following properties:

- (a) if  $\mathcal{C} \subseteq \mathcal{C}'$  then  $V_{\mathcal{C}}(S) \subseteq V_{\mathcal{C}'}(S)$ ,
- (b) if  $S \subseteq S'$  then  $V_{\mathcal{C}}(S') \subseteq V_{\mathcal{C}}(S)$ ,
- (c) if  $T \subseteq T'$  then  $\mathcal{I}(T') \subseteq \mathcal{I}(T)$ ,
- (d)  $S \subseteq \mathcal{I}(V_{\mathcal{C}}(S))$ ,
- (e)  $T \subseteq V_{\mathcal{C}}(\mathcal{I}(T))$ .

□

In addition to shedding light on the basic question of which ideals have the left nullstellensatz property for  $\mathcal{C}$ -points, we would also like to find an algebraic description of the  $\mathcal{C}$ -saturation similar to the notion of real radical in classical real algebraic geometry, see [5, Definition 6.4 and Theorems 6.5 and 6.7] or Example 6.1 below.

These considerations motivate the following definitions. A left ideal  $I$  of  $\mathcal{A}$  is said to be *real* if for every  $a_1, \dots, a_r$  of  $\mathcal{A}$  such that

$$\sum_{i=1}^r a_i^* a_i \in I + I^*,$$

we have that  $a_1, \dots, a_r \in I$ . An intersection of a family of real ideals is a real ideal. For a left ideal  $J$  of  $\mathcal{A}$  we call the ideal

$$\sqrt[\text{rr}]{J} = \bigcap_{I \supseteq J, I \text{ real}} I = \text{the smallest real ideal containing } J$$

the *real radical* of  $J$ . Here are the basic properties.

**Lemma 1.5.** *Let  $\mathcal{C}$  be a representation class and  $I$  a left ideal of  $\mathcal{A}$ .*

*If  $I$  has the left nullstellensatz property for  $\mathcal{C}$ -points, then  $I$  is a real ideal.*

*The  $\mathcal{C}$ -saturation of  $I$  contains the real radical of  $I$ .*

*Proof.* To prove the first claim, suppose  $I$  has the left nullstellensatz property, each of  $a_1, \dots, a_r$  are in  $\mathcal{A}$ ,  $b, c$  are in  $I$  and  $\sum a_j^* a_j = b + c^*$ . Let  $(\pi, v) \in \mathcal{C}$  be given. In particular,  $\pi(b)v = 0 = \pi(c)v$ . Thus,

$$\begin{aligned} \sum \langle \pi(a_j)v, \pi(a_j)v \rangle &= \sum \langle \pi(a_j^* a_j)v, v \rangle \\ &= \langle \pi(b)v, v \rangle + \langle v, \pi(c)v \rangle \\ &= 0. \end{aligned}$$

It follows that  $\pi(a_j)v = 0$  and therefore  $a_j \in \mathcal{I}(V_{\mathcal{R}}(I))$ . Hence, by the left nullstellensatz property,  $a_j \in I$  and  $I$  is a real ideal.

To prove the second claim note that the first claim implies that the smallest left ideal which contains  $I$  and has left nullstellensatz property for  $\mathcal{C}$ -points contains the smallest real left ideal which contains  $I$ . Now use the first claim of Lemma 1.4 and the definition of the real radical to finish the proof.  $\square$

Lemmas 1.4 and 1.5 imply that

$$I \subseteq \sqrt[r]{I} \subseteq \sqrt[r]{I} \subseteq \sqrt[r]{I}$$

for every representation class  $\mathcal{C}$  and every left ideal  $I$  of  $\mathcal{A}$ .

**1.3. Summary of Results.** The main result of this paper is

**Theorem 1.6.**

*A finitely generated left ideal  $I$  in  $F\langle x, x^* \rangle$  satisfies the left nullstellensatz property for  $\Pi$ -points if and only if  $I$  is real. Moreover,*

$$I \subseteq \sqrt[r]{I} = \sqrt[r]{I} = \sqrt[r]{I}.$$

In Section 2, we prove several technical results about the  $*$ -algebra  $F\langle x, x^* \rangle$  which are similar to Gröbner bases computations.

In Section 3 we present an (implementable and effective) algorithm for computing the real radical of a finitely generated left ideal in  $F\langle x, x^* \rangle$ . Its theoretical importance is in the fact that the result is always a finitely generated left ideal. Therefore, the second part of Theorem 1.6 follows from the first.

The first part of Theorem 1.6 is proved in Section 4. The idea is to show that every finitely generated real ideal in  $F\langle x, x^* \rangle$  is of the form  $\{a \in F\langle x, x^* \rangle \mid L(a^*a) = 0\}$  for some positive functional  $L$ .

In Section 5 we shift our attention to general  $*$ -algebras. We prove a topological characterization of the  $\mathcal{R}$ -saturation and develop a (non-effective) iterative procedure for computing the real radical.

In Section 6 we prove that all left ideals  $I$  in  $M_n(F[x_1])$  satisfy  $I \subseteq \sqrt[r]{I} = \sqrt[r]{I} = \sqrt[\varepsilon]{I}$ . The case of several variables remains open.

## 2. IDEALS AND THEIR COMPLEMENTS

In this section we prove a collection of basic facts which constitute the backbone of the main results of this paper. We begin by stating an appealing theorem, Theorem 2.5, which underlies the success of our algorithm given in §3. In the course of its proof we lay out essentials for our main theorem. Recall that  $F$  is  $\mathbb{R}$  or  $\mathbb{C}$  and  $\mathfrak{F} = F\langle x, x^* \rangle$ .

**Definition 2.1.** Let  $\mathfrak{F}_d$  be the vector space spanned by all polynomials in  $\mathfrak{F}$  with degree bounded by  $d$ . In general, given a vector subspace  $V \subseteq \mathfrak{F}$ ,  $V_d$  denotes the space of elements of  $V$  with degree bounded by  $d$ .

**Example 2.2.** If  $V = \mathfrak{F}x_1x_1$ , then  $V_3$  is the space

$$V_3 = \text{span}\{x_1x_1x_1, x_1^*x_1x_1, x_2x_1x_1, x_2^*x_1x_1, x_1x_1\}.$$

□

**Example 2.3.** Let  $x = (x_1, x_2)$  and let  $W = \mathfrak{F}(x_1x_1 + 1)$ . Each element of  $W$  is of the form  $a(x_1x_1 + 1)$  for some  $a \in \mathfrak{F}$ . If  $a$  is nonzero, then the degree of  $a(x_1x_1 + 1)$  is equal to  $2 + \deg(a)$ . Therefore all elements of  $W$  of degree bounded by 3 are of the form

$$W_3 = \{a(x_1x_1 + 1) : \deg(a) \leq 1\}.$$

Therefore  $W_3$  is the spanned by the basis

$$\{x_1(x_1x_1 + 1), x_1^*(x_1x_1 + 1), x_2(x_1x_1 + 1), x_2^*(x_1x_1 + 1), x_1x_1 + 1\}.$$

□

**Definition 2.4.** Let  $V$  be a vector space and let  $W_1$  and  $W_2$  be vector subspaces of  $V$ . If  $W_1 \cap W_2 = (0)$ , let  $W_1 \oplus W_2$  denote the space  $W_1 + W_2 \subseteq V$ . If  $W_1 \cap W_2 \supsetneq (0)$ , then  $W_1 \oplus W_2$  is undefined.

A main result of this section is

**Theorem 2.5.** *Let  $I \subseteq \mathfrak{F}$  be a finitely-generated left ideal. Suppose  $I$  is generated by polynomials  $p_1, \dots, p_k \in \mathfrak{F}$  with  $\deg p_i \leq d$  for each  $i$ . Then the following are equivalent.*

- (1)  $I$  is a real ideal.

- (2) If  $q_1, \dots, q_k$  are polynomials and  $\sum_{i=1}^{\ell} q_i^* q_i \in I + I^*$ , then  $q_j \in I$  for each  $j$ .
- (3) If  $V$  is a subspace of  $\mathfrak{F}_{d-1}$  such that

$$\mathfrak{F}_{d-1} = I_{d-1} \oplus V$$

and  $v_j \in V$  are polynomials such that  $\sum_{i=1}^{\ell} v_i^* v_i \in I + I^*$ , then each  $v_j = 0$ .

The proof of this theorem appears in § 2.1.

An important corollary to Theorem 2.5 is the following.

**Corollary 2.6.** *Let  $I \subseteq \mathfrak{F}$  be a finitely-generated left ideal. Suppose  $I$  is generated by polynomials  $p_1, \dots, p_k \in \mathfrak{F}$  with  $\deg p_i \leq d$  for each  $i$ . Then  $I$  is real if and only if whenever*

$$\sum_{i=1}^{\ell} q_i^* q_i \in I + I^*, \quad \deg(q_1), \dots, \deg(q_{\ell}) < d,$$

then  $q_1, \dots, q_{\ell} \in I$ .

*Proof.* Suppose  $q_1, \dots, q_{\ell}$  have degree less than  $d$  and that

$$\sum_{i=1}^{\ell} q_i^* q_i \in I + I^*.$$

Decompose  $\mathfrak{F}_{d-1}$  as

$$\mathfrak{F}_{d-1} = I_{d-1} \oplus V$$

and express each  $q_i$  as

$$q_i = q_{i,I} + q_{i,V}, \quad q_{i,I} \in I_{d-1}, \quad q_{i,V} \in V.$$

Then

$$\sum_{i=1}^{\ell} q_i^* q_i = \sum_{i=1}^{\ell} (q_{i,I}^* q_i + q_{i,V}^* q_{i,I} + q_{i,V}^* q_{i,V}) \in I + I^*,$$

which implies that

$$(2.1) \quad \sum_{i=1}^{\ell} q_{i,V}^* q_{i,V} \in I + I^*.$$

By Theorem 2.5,  $I$  is real if and only if (2.1) implies that  $q_{i,V} = 0$  for each  $i$ . However, each  $q_i \in I$  if and only if  $q_{i,V} = 0$ . This proves the corollary.  $\square$

**2.1. Proof and Further Facts.** We give a string of facts, which typically involve complements and the degree of polynomials, that underlie proofs of Theorem 2.5.

**Definition 2.7.** Let  $\mathfrak{F}_d^H$  denote the vector space of all homogeneous degree  $d$  polynomials in  $\mathfrak{F}$ . (0 is considered homogeneous of all degrees.) In general, given a vector subspace  $V \subseteq \mathfrak{F}$ ,  $V_d^H$  denotes the space  $V \cap \mathfrak{F}_d^H$  of all homogeneous degree  $d$  elements of  $V$ .

**Example 2.8.** Let  $x = (x_1, x_2)$  so that  $\mathfrak{F} = F\langle x_1, x_2, x_1^*, x_2^* \rangle$ . If  $V = \mathfrak{F}x_1x_1$ , then  $V_3^H$  is the space

$$V_3^H = \text{span}\{x_1x_1x_1, x_1^*x_1x_1, x_2x_1x_1, x_2^*x_1x_1\}.$$

□

**Definition 2.9.** For each nonzero  $p \in \mathfrak{F}$ , the **leading polynomial** of  $p$  is the unique homogeneous polynomial  $p'$  such that  $\deg(p) = \deg(p')$  and  $\deg(p - p') < \deg(p)$ . For a space  $V \subset \mathfrak{F}$ , let  $V_d^\ell$  denote the space spanned by the leading polynomials of all degree  $d$  elements of  $V$ . Note that  $V_d^\ell$  is contained in the space  $\mathfrak{F}_d^H$ .

**Example 2.10.** Let  $x = (x_1, x_2)$  and let  $I = \mathfrak{F}(x_1x_1 + 1) + \mathfrak{F}x_2$ . Then  $I_2$  is the space

$$I_2 = \text{span}\{x_1x_1 + 1, x_1x_2, x_1^*x_2, x_2x_2, x_2^*x_2, x_2\}.$$

The space spanned by all homogeneous degree two polynomials is

$$I_2^H = \text{span}\{x_1x_2, x_1^*x_2, x_2x_2, x_2^*x_2\}.$$

The leading polynomial of  $x_1x_1 + 1$  is  $x_1x_1$  and the leading polynomial of each  $zx_2$  is itself,  $zx_2$ , where  $z = x_1, x_1^*, x_2$ , or  $x_2^*$ . It follows that

$$I_2^\ell = \text{span}\{x_1x_1, x_1x_2, x_1^*x_2, x_2x_2, x_2^*x_2\}.$$

□

**Definition 2.11.** For every pair of subsets  $A$  and  $B$  of  $\mathfrak{F}$  we write  $AB$  for the set of all finite sums of elements of the form  $ab$ ,  $a \in A$ ,  $b \in B$ .

**Example 2.12.** Clearly,  $\mathfrak{F}_k^H \mathfrak{F}_l^H = \mathfrak{F}_{k+l}^H$  for every  $k$  and  $l$ . If  $\mathfrak{F}_l^H = U \oplus V$  for some vector spaces  $U$  and  $V$ , then  $\mathfrak{F}_k^H \mathfrak{F}_l^H = \mathfrak{F}_k^H U \oplus \mathfrak{F}_k^H V$  (since  $\mathfrak{F}_k^H U \cap \mathfrak{F}_k^H V = \{0\}$  by Lemma 2.13.) □

**Lemma 2.13.** Let  $p_1, \dots, p_k \in \mathfrak{F}$  be linearly independent, homogeneous degree  $d$  polynomials. Then

$$q_1p_1 + \dots + q_kp_k = 0$$

for some polynomials  $q_1, \dots, q_k \in \mathfrak{F}$  if and only if each  $q_i = 0$ .



*Proof.* Suppose

$$q_1 p_1 + \dots + q_k p_k = 0$$

for some polynomials  $q_1, \dots, q_k \in \mathfrak{F}$ . Let  $\mathcal{M}$  be a finite set of monomials such that there exist scalars  $A_{m,i}$ , for  $i = 1, \dots, k$ , such that

$$q_i = \sum_{m \in \mathcal{M}} A_{m,i} m.$$

For each  $m \in \mathcal{M}$ ,

$$r_m = \sum_{i=1}^k A_{m,i} p_i$$

is a homogeneous polynomial of degree  $d$ . Since

$$\sum_{m \in \mathcal{M}} m r_m = \sum_{i=1}^k q_i p_i = 0,$$

it follows that  $m r_m = 0$  for all  $m \in \mathcal{M}$ . (This is true because if  $m_1 \neq m_2 \in \mathcal{M}$  then  $m_1 r_{m_1}$  and  $m_2 r_{m_2}$  have disjoint monomials. This in turn is true for the following reason: if  $\deg m_1 \neq \deg m_2$  then they have monomials with different degrees; if  $\deg m_1 = \deg m_2$  then they have monomials with different initial words.) Since all  $r_m$  are 0 and the  $p_i$  are linearly independent, all  $A_{m,i}$  must be 0.  $\square$

**Lemma 2.14.** *Let  $p_1, \dots, p_k \in \mathfrak{F}$  be degree  $d$  polynomials with linearly independent leading polynomials  $p'_1, \dots, p'_k$ . For every  $q_1, \dots, q_k \in \mathfrak{F}$  such that at least one  $q_i$  is nonzero and for every  $u \in \mathfrak{F}_{d-1}$ , the element*

$$q = \sum_{i=1}^k q_i p_i + u$$

*is nonzero, has degree  $d + e$  where  $e = \max\{\deg(q_i) \mid i = 1, \dots, k\}$  and its leading polynomial is  $q' = \sum_{\deg(q_i)=e} q'_i p'_i$ .*

*Proof.* Suppose that at least one  $q_i$  is nonzero. Let  $e = \max_i \{\deg(q_i)\}$ . Let  $\hat{q}'_i = q'_i$  if  $\deg(q_i) = e$  and let  $\hat{q}'_i = 0$  otherwise. Then

$$(2.2) \quad q = \sum_{i=1}^k \hat{q}'_i p'_i + \sum_{i=1}^k (q_i - \hat{q}'_i) p_i + \sum_{i=1}^k \hat{q}'_i (p_i - p'_i) + u.$$

By linear independence of the  $p'_i$  and by Lemma 2.13, the homogeneous polynomial  $\sum_{i=1}^k \hat{q}'_i p'_i$  can only be zero if all of the  $\hat{q}'_i$  equal 0, which

cannot be. Further, each of the other terms of (2.2) must be of degree less than  $d + e$ . Therefore, the leading polynomial of  $q$  is

$$q' = \sum_{i=1}^k \hat{q}'_i p'_i.$$

□

**Lemma 2.15.** *Let  $I \subseteq \mathfrak{F}$  be a left ideal generated by polynomials of degree bounded by  $d$ .*

- (1) *There exist  $p_1, \dots, p_k \in I$  such that  $\deg(p_i) = d$  for each  $i$ , the leading polynomials  $p'_1, \dots, p'_k$  are linearly independent, and  $I$  is equal to*

$$I = \bigoplus_{i=1}^k \mathfrak{F}p_i \oplus I_{d-1}.$$

- (2) *For each  $D \geq d$ , the space  $I_D^\ell$  is equal to*

$$I_D^\ell = \sum_{i=1}^k \mathfrak{F}_{D-d}^H p'_i.$$

*Proof.* First,  $I$  being generated by polynomials of degree bounded by  $d$  implies that  $I = \mathfrak{F}I_d$ . To prove item (1), let  $p_1, \dots, p_k \in I$  be a maximal set of degree  $d$  polynomials in  $I$  such that the leading polynomials  $p'_1, \dots, p'_k$  are linearly independent.

By Lemma 2.13, for any  $a_1, \dots, a_k \in \mathfrak{F}$ , not all equal to 0, we have  $\sum_{i=1}^k a_i p'_i \neq 0$ . Therefore  $\sum_{i=1}^k a_i p_k \neq 0$ , so

$$\sum_{i=1}^k \mathfrak{F}p_i = \bigoplus_{i=1}^k \mathfrak{F}p_i.$$

Further note that each  $\sum_{i=1}^k a_i p_k \neq 0$  must have degree at least  $d$  so that

$$\bigoplus_{i=1}^k \mathfrak{F}p_i \cap I_{d-1} = (0).$$

If  $q \in I$  is any other degree  $d$  polynomial, then by maximality its leading polynomial  $q'$  cannot be linearly independent from the set  $\{p'_1, \dots, p'_k\}$ . Therefore there exist  $\alpha_1, \dots, \alpha_k \in F$  (i.e. scalars) such that

$$q' = \alpha_1 p'_1 + \dots + \alpha_k p'_k.$$

This implies that the polynomial

$$q - \sum_{i=1}^k \alpha_i p_i \in I$$

is either 0 or of degree less than  $d$ . This implies that the set  $I_d$  is equal to

$$I_d = \bigoplus_{i=1}^k Fp_i \oplus I_{d-1}.$$

It now suffices to show that  $\mathfrak{F}I_{d-1} \subseteq \bigoplus_{i=1}^k \mathfrak{F}p_i \oplus I_{d-1}$ .

Proceed by induction on degree to show that for any monomial  $m$  one has  $mI_{d-1} \subseteq \bigoplus_{i=1}^k \mathfrak{F}p_i \oplus I_{d-1}$ . If  $\deg(m) = 0$ , then the result is trivial. Next, suppose the result holds for  $\deg(m) \leq n$ . Let  $m = m_1 m_2$ , where  $\deg(m_2) = 1$ . By the above discussion,  $m_2 I_{d-1} \subseteq I_d = \bigoplus_{i=1}^k \mathfrak{F}p_i \oplus I_{d-1}$ . By induction, since  $\deg(m_1) < \deg(m)$ ,  $m_1 m_2 I_{d-1} \subseteq \bigoplus_{i=1}^k m_1 \mathfrak{F}p_i \oplus m_1 I_{d-1} \subseteq \bigoplus_{i=1}^k \mathfrak{F}p_i \oplus I_{d-1}$ .

For item (2), let  $q \in I$  be a degree  $D$  polynomial. By the first part,

$$q = \sum_{i=1}^k q_i p_i + u,$$

where  $q_1, \dots, q_k \in \mathfrak{F}$  and  $u \in I_{d-1}$ . Since  $D \geq d$ , at least one  $q_i$  is nonzero. Therefore, by Lemma 2.14,  $q' = \sum_{\deg(q_i)=e} q'_i p'_i \in \sum_{i=1}^k \mathfrak{F}_{D-d}^H p'_i$  with  $e = \max_i \{\deg(q_i)\}$ . The converse is clear.  $\square$

Item (2) of Lemma 2.15 says that for every left ideal  $I$  of  $\mathfrak{F}$  generated by elements of degree at most  $d$  and every  $D \geq d$  we have

$$(2.3) \quad I_D^\ell = \mathfrak{F}_{D-d} I_d^\ell.$$

**Lemma 2.16.** *Let  $I \subseteq \mathfrak{F}$  be a left ideal generated by polynomials of degree at most  $d$ . Consider any decomposition of  $\mathfrak{F}_d^H$  of the form*

$$\mathfrak{F}_d^H = I_d^\ell \oplus G,$$

where  $G \subset \mathfrak{F}_d^H$ . Then

$$I \cap \mathfrak{F}G = \mathfrak{F}I_d^\ell \cap \mathfrak{F}G = \{0\}.$$

*Proof.* Suppose  $p \in I \cap \mathfrak{F}G$ . By assertion (1) of Lemma 2.15, there exist  $p_1, \dots, p_k \in I$  of degree  $d$  such that the set of leading terms,  $p'_1, \dots, p'_k$ , is independent and there exist  $q_1, \dots, q_k \in \mathfrak{F}$ ,  $u \in I_{d-1}$  such that  $p = \sum_{i=1}^k q_i p_i + u$ . There also exist a linearly independent set  $v_1, \dots, v_l \in G$  and polynomials  $s_1, \dots, s_l \in \mathfrak{F}$  such that  $p = \sum_{j=1}^l s_j v_j$ . Because  $I_d^\ell \cap G = (0)$ , the set  $p'_1, \dots, p'_k, v_1, \dots, v_l$  is linearly independent. Further,

$0 = p - p = \sum_{i=1}^k q_i p_i + \sum_{j=1} (-s_j) v_j + u$ . By Lemma 2.14 it follows that each  $q_i$  and each  $s_j$  is 0. Hence  $p = \sum s_j v_j = 0$ .

The second equality follows from Example 2.12.  $\square$

**Lemma 2.17.** *Let  $I \subseteq \mathfrak{F}$  be a left ideal generated by polynomials  $p_1, \dots, p_k \in \mathfrak{F}$  with  $\deg p_i \leq d$  for all  $i$ . Suppose  $G$  is a subspace of  $\mathfrak{F}_d^H$  such that*

$$\mathfrak{F}_d^H = I_d^\ell \oplus G.$$

*If  $D \geq d$ , then the space  $(I + I^*)_{2D}^\ell$  is equal to*

$$(2.4) \quad (I + I^*)_{2D}^\ell = [(I_d^\ell)^* \mathfrak{F}_{2(D-d)}^H I_d^\ell] \oplus [G^* \mathfrak{F}_{2(D-d)}^H I_d^\ell] \oplus [(I_d^\ell)^* \mathfrak{F}_{2(D-d)}^H G].$$

*Consequently, the space*

$$W := G^* \mathfrak{F}_{2(D-d)}^H G$$

*satisfies*

$$\mathfrak{F}_{2D}^H = (I + I^*)_{2D}^\ell \oplus W.$$

*Proof.* Each element of  $I + I^*$  is of the form  $p + q^*$ , where  $p, q \in I$ . The leading polynomial of  $p$  is in  $I_{\deg(p)}^\ell$  and the leading polynomial of  $q^*$  is in  $(I_{\deg(q)}^\ell)^*$ . We consider two cases.

First, suppose  $2D = \deg(p + q^*) < \max\{\deg(p), \deg(q)\}$ . This can only happen when the leading polynomials of  $p$  and  $q^*$  cancel each other out, that is, if the leading polynomials of  $p$  and  $-q^*$  are the same. Let  $\deg(p) = \deg(q) = D'$ . Decompose the space  $\mathfrak{F}_{D'}^H$  as

$$(2.5) \quad \begin{aligned} \mathfrak{F}_{D'}^H &= \mathfrak{F}_{D'-d}^H I_d^\ell \oplus \mathfrak{F}_{D'-d}^H G \\ &= [(I_d^\ell \oplus G)^* \mathfrak{F}_{D'-2d}^H I_d^\ell] \oplus [(I_d^\ell \oplus G)^* \mathfrak{F}_{D'-2d}^H G] \\ &= [(I_d^\ell)^* \mathfrak{F}_{D'-2d}^H I_d^\ell] \oplus [H^* \mathfrak{F}_{D'-2d}^H I_d^\ell] \\ &\quad \oplus [(I_d^\ell)^* \mathfrak{F}_{D'-2d}^H G] \oplus [H^* \mathfrak{F}_{D'-2d}^H G]. \end{aligned}$$

Using equations (2.3) and (2.5) respectively, decompose  $I_{D'}^\ell$  as

$$I_{D'}^\ell = \mathfrak{F}_{D'-d}^H I_d^\ell = (I_d^\ell)^* \mathfrak{F}_{D'-2d}^H I_d^\ell \oplus G^* \mathfrak{F}_{D'-2d}^H I_d^\ell,$$

and decompose  $I_{D'}^\ell$  as

$$(I^*)_{D'}^\ell = (I_{D'}^\ell)^* = (I_d^\ell)^* \mathfrak{F}_{D'-2d}^H I_d^\ell \oplus (I_d^\ell)^* \mathfrak{F}_{D'-2d}^H G.$$

The leading polynomial of  $p$  and  $-q^*$  must therefore be in the space

$$I_{D'}^\ell \cap (I^*)_{D'}^\ell = (I_d^\ell)^* \mathfrak{F}_{D'-2d}^H I_d^\ell.$$

Let the leading polynomial of  $p$  and  $-q^*$  be equal to

$$(2.6) \quad p' = -(q')^* = \sum_{i=1}^n (a'_i)^* b_i c'_i \in (I_d^\ell)^* \mathfrak{F}_{D'-2d}^H I_d^\ell$$

where each  $a'_i$  is the leading polynomial of some  $a_i \in I_d$ , each  $c'_i$  is the leading polynomial of some  $c_i \in I_d$ , and  $b_i \in \mathfrak{F}_{D'-2d}^H$ . Then

$$p + q^* = \left( p - \sum_{i=1}^n (a_i)^* b_i c_i \right) + \left( q + \sum_{i=1}^n (c_i)^* (b_i)^* a_i \right)^*,$$

which is a sum of something from  $I$  and something from  $I^*$ , each of degree less than  $D'$ . Proceed inductively to reduce  $p + q^*$  to a sum of polynomials of degree bounded by  $2D$ .

Now consider the case where  $\deg(p), \deg(q) \leq 2D$ . By hypothesis,  $\deg(p + q) = 2D$ , so at least one of  $p$  or  $q$  must be degree  $2D$ . If  $\deg(p) < 2D$ , then  $\deg(q) = 2D$  and the leading polynomial of  $p + q^*$  is the leading polynomial of  $q^*$ , which, by Lemma 2.15, is an element of

$$(I_d^\ell)^* \mathfrak{F}_{2(D-d)} I_d^\ell \oplus (I_d^\ell)^* \mathfrak{F}_{2(D-d)} G.$$

If  $\deg(q) < 2D$ , then  $\deg(p) = 2D$  and the leading polynomial of  $p + q^*$  is the leading polynomial of  $p$ , which, by Lemma 2.15, is an element of

$$(I_d^\ell)^* \mathfrak{F}_{2(D-d)} I_d^\ell \oplus G^* \mathfrak{F}_{2(D-d)} I_d^\ell.$$

If  $\deg(p) = \deg(q) = 2D$ , then the leading polynomial of  $p + q^*$  must be the sum of the leading polynomials of  $p$  and  $q^*$  (which, by assumption, must be nonzero). This is in the space

$$\begin{aligned} & [(I_d^\ell)^* \mathfrak{F}_{2(D-d)} I_d^\ell \oplus (I_d^\ell)^* \mathfrak{F}_{2(D-d)} G] + [(I_d^\ell)^* \mathfrak{F}_{2(D-d)} I_d^\ell \oplus G^* \mathfrak{F}_{2(D-d)} I_d^\ell] \\ &= (I_d^\ell)^* \mathfrak{F}_{2(D-d)} I_d^\ell \oplus H^* \mathfrak{F}_{2(D-d)} I_d^\ell \oplus (I_d^\ell)^* \mathfrak{F}_{2(D-d)} G. \end{aligned}$$

In all cases, the leading polynomial of an element of  $I + I^*$  is in the space (2.4).  $\square$

**Proposition 2.18.** *Let  $I \subseteq \mathfrak{F}$  be a left ideal generated by polynomials with degree bounded by  $d$ .*

(1) *The space  $(I + I^*)_{2d-1}$  is equal to*

$$(I + I^*)_{2d-1} = I_{2d-1} + I_{2d-1}^*.$$

(2) *Choose, by Lemma 2.15 polynomials  $p_1, \dots, p_k$  so that*

$$I = \sum_{i=1}^k \mathfrak{F} p_i + I_{d-1}.$$

*If  $\{q_1, \dots, q_\ell\}$  is a basis for  $I_{d-1}$ , then the set*

$$\begin{aligned} (2.7) \quad & \{mp_i + p_i^* m^* : m \text{ monomial, } \deg(mp_i) < 2d\} \cup \{q_1 + q_1^*, \dots, q_\ell + q_\ell^*\} \\ & \text{spans } (I + I^*)_{2d-1} \cap \mathfrak{F}_h. \end{aligned}$$

*Proof.* Let  $p, q \in I$  with  $\deg(p) \geq 2d$  and  $\deg(p + q^*) < 2d$ . This can only happen if  $\deg(p) = \deg(q)$  and the leading polynomials  $p'$  and  $q'$  of  $p$  and  $q$  respectively satisfy  $(p')^* = -q'$ . As in (2.6), we see that

$$p' = -(q')^* = \sum_{i=1}^n (a'_i)^* b_i c'_i,$$

where  $a'_i, c'_i$  are the leading polynomials of some  $a_i, c_i \in I$ . Therefore

$$p + q^* = \left( p - \sum_{i=1}^n (a_i)^* b_i c_i \right) + \left( q + \sum_{i=1}^n (c_i)^* b_i^* a_i \right)^*,$$

which is a sum of an element of  $I$  of degree less than  $\deg(p)$  and an element of  $I^*$  of degree less than  $\deg(p)$ . We proceed inductively to show that  $p + q^* \in I_{2d-1} + I_{2d-1}^*$ .

Further, by Lemma 2.15  $I_{2d-1}$  is spanned by polynomials of the form  $mp_i$ , with  $m$  a monomial and  $\deg(mp_i) < 2d$ , together with the  $q_j$ . A symmetric polynomial  $p \in I_{2d-1} + I_{2d-1}^*$  is therefore equal to (2.8)

$$p = \sum_{\deg(mp_i) < 2d} A_{mp_i} mp_i + \sum_{\deg(np_j) < 2d} B_{np_j} p_j^* n^* + \sum_{n=1}^{\ell} C_n q_n + \sum_{r=1}^{\ell} D_n q_n^*$$

for some sufficiently defined  $A_{mp_i}, B_{np_j}, C_n \in F$ . But  $p$  being symmetric means  $p = \frac{1}{2}(p + p^*)$ , so

$$p = \frac{1}{2} \left[ \sum A_{mp_i} (mp_i + p_i^* m^*) + \sum B_{np_j} (np_j + p_j^* n^*) + \sum (C_n + D_n)(q_n + q_n^*) \right].$$

Therefore (2.7) is a spanning set for  $(I + I^*)_{2d-1} \cap \mathfrak{F}_h$ .  $\square$

**Lemma 2.19.** *Let  $G$  and  $W$  be as in Lemma 2.17. Let  $q_1, \dots, q_k$  be a basis for  $\mathfrak{F}_{D-d}^H G$ . Then the set of products  $q_i^* q_j$ , where  $1 \leq i, j \leq k$ , is a basis for  $W$ .*

*Proof.* Given that  $q_1, \dots, q_k$  are a basis for  $\mathfrak{F}_{D-d}^H G$ , then

$$\mathfrak{F}_{D-d}^H G = \sum_{i=1}^k F q_i$$

Using Lemma 2.17,

$$W = \left( \sum_{i=1}^k F q_i \right)^* \left( \sum_{i=1}^k F q_i \right) = \sum_{i=1}^k \sum_{j=1}^k F q_i^* q_j.$$

Therefore the  $q_i^* q_j$  span  $W_{2D}^H$ . Further, by Lemma 2.13, the  $q_i^* q_j$  must be linearly independent.  $\square$

The reader who is only interested in the proof of Theorem 1.6 can skip from here to the next section.

**Proposition 2.20.** *If  $I \subseteq \mathfrak{F}$  is a left ideal generated by polynomials of degree at most  $d$ , then there is a subspace  $V$  of  $\mathfrak{F}$  such that*

(1)

$$\mathfrak{F} = I \oplus V,$$

and

$$V = \mathfrak{F}V_d^H \oplus V_{d-1}.$$

In particular,

$$\mathfrak{F}_d^H = I_d^\ell \oplus V_d^H \quad \text{and} \quad \mathfrak{F}_e = I_e \oplus V_e \quad \forall e \geq d-1; \text{ and}$$

(2) if  $\sum_{j=1}^\ell q_j^* q_j \in I + I^*$ , then  $q_i \in I \oplus V_{d-1}$  for each  $j$ .

*Proof.* To prove item (1), first choose a space  $G \subset \mathfrak{F}_d^H$  so that

$$(2.9) \quad \mathfrak{F}_d^H = I_d^\ell \oplus G.$$

By Lemma 2.16,  $I \cap \mathfrak{F}G = (0)$ . Next, choose  $U \subset \mathfrak{F}_{d-1}$  so that  $\mathfrak{F}_{d-1} = I_{d-1} \oplus U$ . In particular  $U \cap I = (0)$ .

Of course  $U \cap \mathfrak{F}G = \emptyset$  because  $U \subset \mathfrak{F}_{d-1}$  and  $\mathfrak{F}G \subset \bigoplus_{i=d}^\infty \mathfrak{F}_i^H$ . Given a word  $m$ , if the degree of  $m$  is  $d$  or less, then evidently  $m \in I_{d-1} \oplus U \subset I \oplus \mathfrak{F}G \oplus U$ . If the degree of  $m$  exceeds  $d$ , then  $m = pw$  where  $w$  is a word of length  $d$  and  $p$  is a word. By equation (2.9),  $w = h' + g$  for some  $h' \in I_d^\ell$  and some  $g \in G$ . Let  $h \in I_d$  be such that the leading polynomial of  $h$  is  $h'$  so that  $h' - h \in \mathfrak{F}_{d-1}$ . Thus,  $ph \in I$  and  $pg \in \mathfrak{F}G$  and it follows that  $m = ph + pg + p(h' - h) \in I \oplus \mathfrak{F}G \oplus \mathfrak{F}_{d-1}$ . Consequently,

$$\mathfrak{F} = I \oplus \mathfrak{F}G \oplus U.$$

Let  $V$  be equal to

$$V = \mathfrak{F}G \oplus U.$$

The space  $\mathfrak{F}G$  has polynomials whose terms have degree at least  $d$ , whereas the space  $U$  has polynomials of degree less than  $d$ . Therefore  $U = V_{d-1}$ . Further, this implies that  $V_d^H$  must be contained in  $\mathfrak{F}G$ . The homogeneous degree  $d$  polynomials in  $\mathfrak{F}G$  are precisely those in  $G$ . Therefore  $G = V_d^H$ .

Turning to item (2), suppose there exists a sum of squares  $\sum_{j=1}^\ell q_j^* q_j \in I + I^*$ . Decompose each  $q_j$  as

$$q_j = q_{j,I} + q_{j,\mathfrak{F}V_d^H} + q_{j,V_{d-1}}$$

where  $q_{j,W} \in W$  for each space  $W$  used. This implies

$$\begin{aligned} \sum_{j=1}^{\ell} q_j^* q_j &= \sum_{j=1}^{\ell} (q_{j,I} + q_{j,\mathfrak{F}V_d^H} + q_{j,V_{d-1}})^* (q_{j,I} + q_{j,\mathfrak{F}V_d^H} + q_{j,V_{d-1}}) \\ (2.10) \quad &= \sum_{i=1}^{\ell} \left[ (q_{i,I} + q_{i,\mathfrak{F}V_d^H} + q_{i,V_{d-1}})^* q_{i,I} + q_{i,I}^* (q_{i,\mathfrak{F}V_d^H} + q_{i,V_{d-1}}) \right] \end{aligned}$$

$$(2.11) \quad + \sum_{j=1}^{\ell} (q_{j,\mathfrak{F}V_d^H} + q_{j,V_{d-1}})^* (q_{j,\mathfrak{F}V_d^H} + q_{j,V_{d-1}}) \in I + I^*.$$

Since (2.10) is in  $I + I^*$ , this implies that 2.11 is in  $I + I^*$ .

Assume

$$\sum_{j=1}^{\ell} (q_{j,\mathfrak{F}V_d^H})^* (q_{j,\mathfrak{F}V_d^H}) \neq 0$$

Suppose  $\sum_{j=1}^{\ell} (q_{j,\mathfrak{F}V_d^H})^* (q_{j,\mathfrak{F}V_d^H})$  is degree  $2D$ , for  $D \geq d$ , and let each  $q_{j,\mathfrak{F}V_d^H}$  be equal to

$$q_{j,\mathfrak{F}V_d^H} = v_j + w_j,$$

where  $v_j \in \mathfrak{F}_{D-d}^H V_d^H$  and where  $\deg(w_j) < D$ . Also, by definition each  $q_{j,V_{d-1}}$  must have degree less than  $d$ . Therefore

$$\begin{aligned} \sum_{j=1}^{\ell} (q_{j,\mathfrak{F}V_d^H} + q_{j,V_{d-1}})^* (q_{j,\mathfrak{F}V_d^H} + q_{j,V_{d-1}}) &= \sum_{j=1}^{\ell} v_j^* v_j \\ (2.12) \quad &+ \sum_{i=1}^{\ell} \left[ (v_i + w_i + q_{i,V_{d-1}})^* (w_i + q_{i,V_{d-1}}) + (w_i + q_{i,V_{d-1}})^* v_i \right] \end{aligned}$$

We see that (2.12) has degree less than  $2D$  and that

$$\sum_{j=1}^{\ell} v_j^* v_j \in \mathfrak{F}_{2D}^H.$$

Therefore the leading polynomial of (2.11) is

$$\sum_{j=1}^{\ell} v_j^* v_j \in (V_d^H)^* \mathfrak{F}_{2(D-d)}^H V_d^H.$$

Since (2.11) is in the space  $I + I^*$ , this implies that

$$\sum_{j=1}^{\ell} v_j^* v_j \in (I + I^*)_{2D}^{\ell}.$$



By Lemma 2.17 and by the decomposition of  $\mathfrak{F}_{D'}^H$  in (2.5), this implies that

$$\sum_{j=1}^{\ell} v_j^* v_j \in (I + I^*)_{2D}^{\ell} \cap (V_d^H)^* \mathfrak{F}_{2(D-d)}^H V_d^H = (0).$$

This implies that each  $v_j = 0$ , which is a contradiction. Therefore each  $q_{j,V_d^H} = 0$ , which implies that each  $q_i \in I \oplus V_{d-1}$ .  $\square$

With these lemmas, we proceed to prove Theorem 2.5.

## 2.2. Proof of Theorem 2.5.

*Proof.* The direction (1)  $\Rightarrow$  (2) follows by definition, and the direction (2)  $\Rightarrow$  (3) is clear.

Assume (3). Decompose  $\mathfrak{F}_{d-1}$  as

$$\mathfrak{F}_{d-1} = I_{d-1} \oplus V$$

for some space  $V$ . Decompose  $\mathfrak{F}_d^H$  as

$$\mathfrak{F}_d^H = I_d^{\ell} \oplus V_d^H$$

for some space  $V_d^H \subset \mathfrak{F}_d^H$ . Then as in Proposition 2.20,

$$\mathfrak{F} = I \oplus \mathfrak{F}_d^H \oplus V,$$

where  $V$  takes the place of  $V_{d-1}$ .

Suppose

$$\sum_{j=1}^k q_j^* q_j \in I + I^*.$$

By Proposition 2.20, each  $q_j \in I \oplus V$ . Let each  $q_i$  be equal to

$$q_j = \iota_j + v_j,$$

where  $\iota_j \in I$  and  $v_j \in V$ . Then

$$\begin{aligned} \sum_{j=1}^k q_j^* q_j &= \sum_{i=1}^{\ell} v_i^* v_i \\ (2.13) \quad &+ \sum_{j=1}^k [\iota_j^* v_j + v_j^* \iota_j + \iota_j^* \iota_j]. \end{aligned}$$

The line (2.13) is in  $I + I^*$ , which implies that  $\sum_{i=1}^{\ell} v_i^* v_i \in I + I^*$ . By (3), each  $v_i$  must be equal to 0. Therefore  $q_j = \iota_j \in I$  for each  $j$ . This implies (1).  $\square$

### 3. AN ALGORITHM FOR COMPUTING $\sqrt[r]{I}$

It is of interest to describe and to compute the real radical of a left ideal  $I$ , in part because of its close relation to the  $\Pi$ -saturation of  $I$ . This section gives an algorithm and theory which shows that the algorithm does indeed have very desirable properties.

**3.1. The Real Algorithm.** The following is an algorithm for computing  $\sqrt[r]{I}$  given a finitely-generated left ideal  $I \subset \mathfrak{F}$ . Here, let  $I = \sum_{i=1}^k \mathfrak{F}p_i$ , where the  $p_i \in \mathfrak{F}$  are polynomials with  $\deg p_i \leq d$ .

- (1) Let  $I^{(0)} = I$ .
- (2) At each step  $k$  we have an ideal  $I^{(k)} \subset \sqrt[r]{I}$  generated by polynomials of degree bounded by  $d$ . Find a sum of squares  $\sum_{i=1}^n q_i^* q_i \in I^{(k)} + I^{(k)*}$  such that for each  $j$  one has  $q_j \notin I$  and  $\deg(q_j) < d$ . If such a sum of squares is not obvious, the following algorithm, which we will refer to as the **SOS Algorithm**, either computes such a sum of squares or proves that none exists.

#### SOS Algorithm

- (a) Find a complementary space  $V^{(k)} \subset \mathfrak{F}_{d-1}$  such that

$$\mathfrak{F}_{d-1} = I_{d-1}^{(k)} \oplus V^{(k)}.$$

Find a basis  $\{v_1, \dots, v_\ell\}$  for  $V^{(k)}$ .

- (b) Parameterize the symmetric elements of  $I^{(k)} + I^{(k)*}$  which appear in the span of  $\{v_i^* v_j\}$  as

$$\begin{pmatrix} v_1 \\ \vdots \\ v_\ell \end{pmatrix}^T (\alpha_1 A_1 + \dots + \alpha_m A_m) \begin{pmatrix} v_1 \\ \vdots \\ v_\ell \end{pmatrix},$$

for some Hermitian matrices  $A_i \in F^{\ell \times \ell}$ .

- To find the matrices  $A_1, \dots, A_m$ , one does the following.

Find a basis  $\iota_1, \dots, \iota_p$  for the symmetric elements of

$$(I^{(k)} + I^{(k)*})_{2d-2}.$$

The set (2.7) in Proposition 2.18 gives a spanning set from which one can choose a maximal linearly independent subset. Solve the equation

$$(3.1) \quad \begin{pmatrix} v_1 \\ \vdots \\ v_\ell \end{pmatrix}^T \begin{pmatrix} a_{11} & \dots & a_{1\ell} \\ \vdots & \ddots & \vdots \\ a_{\ell 1} & \dots & a_{\ell\ell} \end{pmatrix} \begin{pmatrix} v_1 \\ \vdots \\ v_\ell \end{pmatrix} = \alpha_1 \iota_1 + \dots + \alpha_p \iota_p.$$

This amounts to solving a system of linear equations in variables  $a_{ij}$  and  $\alpha_j$ , which system is given by setting the coefficient of each monomial in (3.1) equal to zero. Project this set of solutions onto the coordinates  $a_{ij}$  to get the set

$$\{A = (a_{ij})_{1 \leq i, j \leq \ell} \mid \exists \alpha_1, \dots, \alpha_m : (3.1) \text{ holds}\}.$$

Find a basis  $A_1, \dots, A_m$  for this new projected space.

(c) Solve the following linear matrix inequality for  $(\alpha_1, \dots, \alpha_m)$ .

$$\alpha_1 A_1 + \dots + \alpha_m A_m \succeq 0 \quad \text{and} \quad (\alpha_1, \dots, \alpha_m) \neq 0.$$

- If there is a solution  $(\alpha'_1, \dots, \alpha'_m) \neq 0$ , then let  $q_1, \dots, q_n$  be the polynomials

$$\begin{pmatrix} q_1 \\ \vdots \\ q_n \end{pmatrix} = \sqrt{\alpha'_1 A_1 + \dots + \alpha'_m A_m} \begin{pmatrix} v_1 \\ \vdots \\ v_\ell \end{pmatrix}.$$

Then  $\sum_{i=1}^n q_i^* q_i \in I^{(k)} + I^{(k)*}$  is such that each  $q_j \notin I$  and  $\deg q_j < d$ .

- If this linear matrix inequality has no solution, then there exists no sum of squares  $\sum_{i=1}^n q_i^* q_i \in I^{(k)} + I^{(k)*}$  such that each  $q_j \notin I$  and  $\deg q_j < d$ .
- (3) If there exists a sum of squares  $\sum_{i=1}^n q_i^* q_i \in I^{(k)} + I^{(k)*}$  such that each  $q_j \notin I$  and  $\deg q_i < d$ , then let  $I^{(k+1)} = I^{(k)} + \sum_{i=1}^n \mathfrak{F} q_i$ , let  $k = k + 1$ , note that  $I^{(k+1)}$  is again an ideal, and go to step 2.
  - (4) If there exists no sum of squares  $\sum_{i=1}^n q_i^* q_i \in I^{(k)} + I^{(k)*}$  such that each  $q_j \notin I$  and  $\deg q_j < d$ , then output  $I^{(k)}$  and end the Algorithm.

□

The following theorem presents some appealing properties of the Real Algorithm.

**Theorem 3.1.** *Let  $I$  be the left ideal generated by polynomials  $p_1, \dots, p_k$ , with  $\deg(p_i) \leq d$  for each  $i$ . The following are true for applying the Algorithm described in §3.1 to  $I$ .*

- (1) *This Algorithm involves only computations of polynomials which have degree less than  $d$ .*
- (2) *The Algorithm is guaranteed to terminate in a finite number of steps.*
- (3) *When the Real Algorithm terminates, it outputs the ideal  $\sqrt[3]{I}$ .*

*Proof.* (1) This is clear from the steps of the Algorithm.

- (2) In the Algorithm, at each step the ideal  $I^{(k+1)} = I^{(k)} + \sum_{i=1}^n \mathfrak{F}q_i$  is formed from some polynomials  $q_i$  with degree bounded by  $d-1$ . The chain  $I_{d-1}^{(k)}$  is strictly increasing and hence, in view of item 1,

$$I_{d-1}^{(0)} \subsetneq I_{d-1}^{(1)} \subsetneq I_{d-1}^{(2)} \subsetneq \cdots.$$

Since each  $I_{d-1}^{(k)}$  is a subset of the finite dimensional vector space  $\mathfrak{F}_{d-1}$ , this chain, and thus the Algorithm, terminates.

- (3) First of all,  $I^{(0)} \subset \sqrt[r]{I}$ . Suppose by induction that  $I^{(k)} \subset \sqrt[r]{I}$ . If there exists a sum of squares  $\sum_{i=1}^n q_i^* q_i \in I^{(k)}$  such that  $q_i \notin I$  for each  $i$ , it follows that

$$\sum_{i=1}^n q_i^* q_i \in I^{(k)} \subset \sqrt[r]{I}.$$

This implies that  $q_i \in \sqrt[r]{I}$  for each  $i$ . Therefore

$$I^{(k)} + \sum_{i=1}^n \mathfrak{F}q_i \subseteq \sqrt[r]{I}.$$

Continue this process until there is an  $I^{(k')} \subset \sqrt[r]{I}$  such that there exists no such sum of squares. By Theorem 2.5, the left ideal  $I^{(k')}$  is real, and hence equal to  $\sqrt[r]{I}$ . The algorithm also stops at this point, and so  $\sqrt[r]{I}$  is the output.  $\square$

**3.2. An Example of Applying the Algorithm.** We apply the Algorithm on the left ideal

$$I = \mathfrak{F}([x_1^* x_1 + x_2 x_3 x_3^* x_2^*]^* [x_1^* x_1 + x_2 x_3 x_3^* x_2^*] + x_4^* x_4).$$

We see that

$$p := [x_1^* x_1 + x_2 x_3 x_3^* x_2^*]^* [x_1^* x_1 + x_2 x_3 x_3^* x_2^*] + x_4^* x_4$$

is in  $I$  and is a sum of squares. We take  $q_1 = x_1^* x_1 + x_2 x_3 x_3^* x_2^*$  and  $q_2 = x_4$ , which have degree less than 8, to form the ideal  $I^{(1)}$  equal to

$$I^{(1)} = \mathfrak{F}(x_1^* x_1 + x_2 x_3 x_3^* x_2^*) + \mathfrak{F}x_4.$$

Note  $I^{(0)} \subset I^{(1)}$ .

In  $I^{(1)}$  there is a sum of squares

$$x_1^* x_1 + x_2 x_3 x_3^* x_2^* \in I^{(1)}.$$

The ideal  $I^{(2)}$  is constructed similarly and is

$$I^{(2)} = \mathfrak{F}x_1 + \mathfrak{F}x_3^* x_2^* + \mathfrak{F}x_4.$$

At this point it may not be obvious that whether or not there is a nontrivial sum of squares in  $I^{(2)} + I^{(2)*}$ . We turn to the SOS Algorithm to either find such a sum of squares or prove that one does not exist.

Since  $I^{(2)}$  is generated by polynomials of degree bounded by two, let  $d = 2$ .

*Step 2a.* First we find a complementary space  $V^{(2)}$ . The space  $I_1^{(2)}$  is the span

$$I_1^{(2)} = \text{span}\{x_1, x_4\}.$$

Choose  $V^{(2)}$  to be

$$V^{(2)} = \text{span}\{x_1^*, x_2, x_2^*, x_3, x_3^*, x_4^*, 1\}$$

so that  $\mathfrak{F}_1 = I_1^{(2)} \oplus V^{(2)}$ .

*Step 2b.* Elements of  $I^{(2)} + I^{(2)*}$  are sums of monomials with the rightmost letters being  $x_1, x_3^*x_2^*$  or  $x_4$ , or the leftmost letters being  $x_1^*, x_2x_3$  or  $x_4^*$ . Because  $x_1, x_4 \notin V^{(2)}$ , the only such polynomials in the span of the  $v_i^*v_j$  are polynomials of the form  $\alpha x_3^*x_2^* + \beta x_2x_3$ , where  $\alpha, \beta \in F$ . Consequently, the only symmetric elements of  $I^{(2)} + I^{(2)*}$  in  $\text{span}\{v_i^*v_j\}$  are polynomials of the form  $\alpha(x_3^*x_2^* + x_2x_3)$ , with  $\alpha \in F$ .

*Step 2c.* We then parameterize all elements of  $(I^{(2)} + I^{(2)*}) \cap \text{span}\{v_i^*v_j\}$  as

$$\alpha \begin{pmatrix} x_1^* \\ x_2 \\ x_2^* \\ x_3 \\ x_3^* \\ x_4^* \\ 1 \end{pmatrix}^* \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} x_1^* \\ x_2 \\ x_2^* \\ x_3 \\ x_3^* \\ x_4^* \\ 1 \end{pmatrix}$$

The linear matrix inequality

$$\alpha \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \succeq 0$$

has no nonzero solution in  $\alpha$  since the matrix in question is neither positive semi-definite nor negative semi-definite. This means we go to Step 4 of the Algorithm which says stop. Therefore

$$\sqrt[{\text{rr}}]{I} = \mathfrak{F}x_1 + \mathfrak{F}x_3^*x_2^* + \mathfrak{F}x_4.$$

□

#### 4. A NULLSTELLENSATZ FOR $F\langle x, x^* \rangle$

We provide the remaining ingredients for the proof of Theorem 1.6, namely Theorem 4.1 and Proposition 4.2. The proof also depends on the Real Algorithm.

**4.1. Existence of Positive Linear Functionals.** The following is the main technical result used in the proof of Theorem 1.6.

**Theorem 4.1.** *Let  $I$  be a finitely-generated real left ideal. Then there exists a positive hermitian  $F$ -linear functional  $L$  on  $\mathfrak{F}$  such that*

$$I = \{a \in \mathfrak{F} \mid L(a^*a) = 0\}.$$

*Proof.* Let  $I$  be generated by a set of polynomials with degree bounded by  $d$ . We will first construct a linear functional  $L$  on  $\mathfrak{F}_{2d-2}$  such that

- (i)  $L((I + I^*) \cap \mathfrak{F}_{2d-2}) = 0$ ,
- (ii)  $L(a^*a) > 0$  for every  $a \in \mathfrak{F}_{d-1} \setminus I$  and
- (iii)  $L(a^*) = L(a)^*$  for every  $a \in \mathfrak{F}_{2d-2}$ .

Choose, by Proposition 2.20, a subspace  $V$  of  $\mathfrak{F}$  such that

$$\mathfrak{F} = I \oplus \mathfrak{F}V_d^H \oplus V_{d-1}.$$

and

$$(4.1) \quad \mathfrak{F}_e = I_e \oplus V_e$$

for each  $e \geq d-1$ . Let  $q_1, \dots, q_k$  span  $V_{d-1}$ , and let  $q = (q_1, \dots, q_k)$ .

Let  $M_k(F)_h$  be the set of all hermitian  $k \times k$  matrices with entries in  $F$ . (If  $F = \mathbb{R}$ , then this is the set of symmetric matrices in  $M_k(\mathbb{R})$ .) The real vector space  $M_k(F)_h$  carries the (real-valued) inner product  $\langle C, D \rangle = \text{Tr}(CD)$ .

Let  $B_1, \dots, B_k$  be an orthonormal basis for the subspace  $\{B \in M_k(F)_h \mid q^*Bq \in I + I^*\}$  and let  $A_1, \dots, A_m$  be its completion to an orthonormal basis for  $M_k(F)_h$ . Consider  $M(\alpha, \beta)$  defined by

$$M(\alpha, \beta) = \sum_{i=1}^m \alpha_i A_i + \sum_{j=1}^k \beta_j B_j, \quad \alpha \in \mathbb{R}^m, \beta \in \mathbb{R}^k.$$

Since the  $A_i$  and  $B_j$  form a basis for  $M_k(F)_h$ , the function  $M(\alpha, \beta): \mathbb{R}^m \times \mathbb{R}^k \rightarrow M_k(F)_h$  is onto. Therefore the set  $\mathcal{C}$  defined by

$$\mathcal{C} = \{\beta \in \mathbb{R}^k \mid \exists \alpha: M(\alpha, \beta) \succ 0\}$$

is a nonempty convex set.

If  $0 \notin \mathcal{C}$ , then there exists  $x \neq 0$  such that

$$\mathcal{C} \subset \{y \mid \langle x, y \rangle \geq 0\}.$$

Let  $B = \sum_{j=1}^k x_j B_j$ . Then for each positive definite matrix in  $M_k(F)_h$  which, since  $M$  is onto, must be of the form  $M(\alpha, \beta)$  for some  $\alpha, \beta$ ,

$$\langle M(\alpha, \beta), B \rangle = \langle x, \beta \rangle \geq 0.$$

Therefore the matrix  $B \succeq 0$ . This is a contradiction since  $I$  is real, but  $q^* B q$  is a sum of squares in  $I + I^*$  of elements which are not in  $I$ . Therefore,  $0 \in \mathcal{C}$ , which implies that there exists  $A = \sum_{i=1}^m \alpha_i A_i \succ 0$ .

This  $A$  is the key to the construction of  $L$ . Note that  $\langle A, B \rangle = 0$  for every  $B \in M_k(F)_h$  such that  $q^* B q \in I + I^*$ . To show that if fact  $\text{Tr}(AB) = 0$  whenever  $B \in M_k(F)$  and  $q^* B q \in I + I^*$ , we consider two cases depending on the base field  $F$ . If  $F = \mathbb{R}$ , then  $q^*(B + B^*)q \in I + I^*$  so

$$2 \text{Tr}(AB) = \langle A, B + B^* \rangle = 0.$$

If  $F = \mathbb{C}$ , then  $q^*(B + B^*)q$  and  $q^*(iB - iB^*)q$  are both in  $I + I^*$  so

$$2 \text{Tr}(AB) = \langle A, B + B^* \rangle - i \langle A, iB - iB^* \rangle = 0.$$

Next, note that, using equation (4.1),

$$\mathfrak{F}_{2d-2} = \mathfrak{F}_{d-1}^* \mathfrak{F}_{d-1} = I_{d-1}^* I_{d-1} + I_{d-1}^* V_{d-1} + V_{d-1}^* I_{d-1} + V_{d-1}^* V_{d-1}.$$

Therefore each  $p \in \mathfrak{F}_{2d-1}$  can be expressed as  $p = \iota + q^* B q$ , where  $\iota \in I_{2d-2} + I_{2d-2}^*$  and  $B \in M_k(F)$ . Define  $L$  on  $\mathfrak{F}_{2d-2}$  to be

$$L(p) = L(\iota + q^* B q) = \text{Tr}(AB).$$

In particular,  $L((I + I^*)_{2d-2}) = \{0\}$ . If  $p$  can also be expressed as  $p = \tilde{\iota} + q^* \tilde{B} q$ , with  $\tilde{\iota} \in I_{2d-2} + I_{2d-2}^*$  and  $\tilde{B} \in M_k(F)$ , then  $\tilde{\iota} - \iota = q^*(B - \tilde{B})q \in I + I^*$ . By the previous paragraph,  $\text{Tr}(A(B - \tilde{B})) = 0$ , which implies that  $L$  is well-defined. Also, we see

$$L([\iota + q^* B q]^*) = \text{Tr}(AB^*) = \text{Tr}(AB)^* = L(\iota + q^* B q)^*.$$

Finally, if  $a \in \mathfrak{F}_{d-1} \setminus I_{d-1}$ , then an application of equation (4.1) shows  $a = a_I + \alpha^* q$ , for some  $a_I \in I_{d-1}$ , and  $0 \neq \alpha \in F^k$ . Since  $A \succ 0$ ,

$$L(a^* a) = L(q^* \alpha \alpha^* q) = \text{Tr}(A \alpha \alpha^*) = \alpha^* A \alpha > 0.$$

Next we extend  $L$  inductively by degree. Suppose that  $L$  is defined on  $\mathfrak{F}_{2D-2}$ ,  $D \geq d$ , and it satisfies properties (i)-(iii) with  $d$  replaced by  $D$ . We set about to extend  $L$  to  $\mathfrak{F}_{2D}$ . The extension will satisfy properties (i)-(iii) with  $d$  replaced by  $D + 1$ .

First we address degree  $2D - 1$ . Write the disjoint decomposition of the space where we must define our extended  $L$  as

$$\mathfrak{F}_{2D-1}^H = (I + I^*)_{2D-1}^\ell \oplus W_{2D-1}^H.$$

for some subspace  $W_{2D-1}^H$ . We define  $L$  to be 0 on  $W_{2D-1}^H$  and turn to defining  $L$  on  $(I + I^*)_{2D-1}^\ell$  so as to meet the key constraint  $L((I + I^*)_{2D-1}) = \{0\}$ .

Let  $p'$  be in  $(I + I^*)_{2D-1}^\ell$ , and let  $p \in (I + I^*)_{2D-1}$  be such that  $p'$  is the leading polynomial of  $p$ . Define  $L(p')$  to be  $L(p' - p)$ . To prove that  $L(p')$  is well-defined suppose that  $p'$  is also the leading polynomial of some  $\tilde{p} \in (I + I^*)_{2D-1}$ . The polynomial  $p - \tilde{p}$  clearly belongs to  $(I + I^*)_{2D-2}$ , hence  $L(p - \tilde{p}) = 0$  by assumption. It follows that  $L(p' - p) = L(p' - \tilde{p})$ . The definition of  $L(p')$  implies that  $L(p) = L(p') + L(p - p') = 0$  for every  $p \in (I + I^*)_{2D-1}$ . Also note that

$$L[(p')^*] = L[(p')^* - p^*] = L[p' - p]^* = L[p']^*.$$

Next we extend  $L$  to degree  $2D$ . As in the degree  $2D - 1$  case,  $L$  can be extended to  $(I + I^*)_{2D}^\ell$  to make  $L((I + I^*)_{2D}) = \{0\}$ .

By Lemma 2.17,

$$\mathfrak{F}_{2D}^H = (I + I^*)_{2D}^\ell \oplus W_{2D}^H$$

where

$$W_{2D}^H := (V_d^H)^* \mathfrak{F}_{2(D-d)}^H V_d^H$$

It follows from Lemma 2.16 that

$$\mathfrak{F}_D^H = I_D^\ell \oplus V_D^H.$$

Note  $V_D^H = \mathfrak{F}_{D-d}^H V_d^H$ . Let  $r_1, \dots, r_k$  be a basis for  $V_D^H$ . By Lemma 2.19, the set of products  $r_i^* r_j$  is a basis for  $W_{2D}^H$ . For these basis elements, define  $L$  to be  $L(r_i^* r_i) = c$ , where  $c > 0$  is yet to be determined, and  $L(r_i^* r_j) = 0$  for  $i \neq j$ . Clearly,  $L(a^*) = L(a)^*$  for every  $a \in \mathfrak{F}_{2D}$ .

By Proposition 2.20,

$$\mathfrak{F}_D = I_D \oplus V_D \quad \text{and} \quad V_D = V_D^H \oplus V_{D-1}.$$

Let  $r_{k+1}, \dots, r_n$  be a basis for  $V_{D-1}$  so that  $r_1, \dots, r_n$  is a basis for  $V_D$ . Let  $r = (r_1, \dots, r_k)$  and  $\bar{r} = (r_{k+1}, \dots, r_n)$ . If  $a \in \mathfrak{F}_D \setminus I_D$ , then  $a$  is of the form  $a = \iota + \alpha^* r + \bar{\alpha}^* \bar{r}$  for some  $\iota \in I$ ,  $\alpha \in F^k$ ,  $\bar{\alpha} \in F^{n-k}$ , and at least one of  $\alpha$  and  $\bar{\alpha}$  is nonzero. We see

$$L(a^* a) = \begin{bmatrix} \alpha^* & \bar{\alpha}^* \end{bmatrix} \begin{bmatrix} cI_k & R \\ R^* & S \end{bmatrix} \begin{bmatrix} \alpha \\ \bar{\alpha} \end{bmatrix},$$

where the  $ij^{th}$  entry of  $S$  is  $L(r_{k+i}^* r_{k+j})$  and the  $ij^{th}$  entry of  $R$  is  $L(r_{k+i}^* r_j)$ . Therefore  $L(a^* a) > 0$  for all  $a \in \mathfrak{F}_D \setminus I_D$  if and only if the matrix  $\begin{bmatrix} cI_k & R \\ R^* & S \end{bmatrix}$  is positive definite. Note that if  $\bar{\alpha} \neq 0$ , then from an induction hypothesis,

$$\bar{\alpha}^* S \bar{\alpha} = L((\bar{\alpha}^* \bar{r})^* (\bar{\alpha}^* \bar{r})) > 0$$



since  $\bar{\alpha}^* \bar{r} \in \mathfrak{F}_{D-1} \setminus I_{D-1}$ . Therefore  $S \succ 0$ . The last step in defining  $L$  therefore is to pick  $c$  sufficiently large such that the matrix  $\begin{bmatrix} cI_k & R \\ R^* & S \end{bmatrix}$  is positive definite.  $\square$

**4.2. Relation between  $\sqrt[n]{I}$  and  $\sqrt[r]{I}$ .** We will show that  $\sqrt[n]{I} = \sqrt[r]{I}$  for finitely generated left ideals  $I$  in  $F\langle x, x^* \rangle$ .

**Proposition 4.2.** *If  $p_1, \dots, p_k \in F\langle x, x^* \rangle$  and  $I = \sum_{i=1}^k F\langle x, x^* \rangle p_i$ , then*

$$\sqrt[n]{I} = \sqrt[r]{I}$$

*In particular, suppose  $q \in F\langle x, x^* \rangle$  is such that for each  $\Pi$ -point  $(X', v')$  such that*

$$p_1(X')[v'] = p_2(X')[v'] = \dots = p_k(X')[v'] = 0$$

*that  $q(X')[v'] = 0$ . Then for each  $\mathcal{R}$ -point  $(X, v)$  such that*

$$p_1(X)[v] = p_2(X)[v] = \dots = p_k(X)[v] = 0,$$

*then  $q(X)[v] = 0$  also.*

Recall that  $\Pi$ -points are, loosely speaking, finite-dimensional representations and  $\mathcal{R}$ -points include infinite-dimensional representations.

*Proof.* Suppose  $q \in F\langle x, x^* \rangle$ , and let  $d = \max\{\deg(p_1), \dots, \deg(p_k), q\}$ . Let  $(X, v)$  a representation on some pre-Hilbert space  $\mathcal{H}$ . Define  $V$  to be the space

$$V = \{p(X)[v] : \deg(p) \leq d\} \subset \mathcal{H}.$$

Since the space of polynomials with degree less than or equal to  $d$  is finite dimensional, it follows that  $V$  is also finite dimensional. Define  $X' : V^g \rightarrow V$  by

$$X' = (P_V X_1 P_V, \dots, P_V X_g P_V).$$

Note that  $(P_V X_j P_V)^* = P_V X_j^* P_V$ . We claim that for each  $r \in F\langle x, x^* \rangle$  of degree at most  $d$ ,

$$(4.2) \quad r(X')[v] = r(X)[v].$$

Proceed by induction on  $\deg(r)$ . If  $r$  is a constant, then  $r(X')[v] = rv = r(X)[v]$ . Next, consider the case where  $r$  is monomial of degree  $j \leq d$ . Let  $r$  be expressed as

$$r = ym$$

where  $y$  is a variable, i.e.  $\deg(y) = 1$ , and where  $m$  is a monomial of degree  $j - 1$ . Assume inductively that  $m(X')[v] = m(X)[v]$ . Note that  $m(X)[v] \in V$  since  $\deg(m') \leq d$ . Therefore

$$\begin{aligned} r(X')[v] &= y(X')m(X')[v] = P_V y(X) P_V m(X')[v] = \\ &= P_V y(X) P_V m(X)[v] = P_V y(X) m(X)[v] = P_V r(X)[v], \end{aligned}$$

where  $y(X)$  denotes evaluating the polynomial  $y$  at the  $g$ -tuple  $X$ . Since  $\deg(r) \leq d$ , by definition  $r(X)[v] \in V$ , so  $r(X')[v] = r(X)[v]$ . By induction and by linearity, this implies that for any  $r \in F\langle x, x^* \rangle$  with  $\deg(r) \leq d$ , equation (4.2) holds.

Suppose  $q \in \sqrt[n]{I}$ . If

$$p_1(X)[v] = p_2(X)[v] = \dots = p_k(X)[v] = 0,$$

then

$$p_1(X')[v] = p_2(X')[v] = \dots = p_k(X')[v] = 0.$$

Since  $(X', v)$  is a finite-dimensional representation, this implies that

$$q(X)[v] = q(X')[v] = 0.$$

Therefore,  $q \in \sqrt[r]{I}$ . □

#### 4.3. Proof of Theorem 1.6.

*Proof.* Let  $I$  be a finitely generated left ideal in  $\mathfrak{F} = F\langle x, x^* \rangle$ . Then

$$\sqrt[r]{I} = \sqrt[n]{I}$$

by Proposition 4.2. By Theorem 3.1, the real left ideal

$$J := \sqrt[v]{I}$$

is finitely generated. Then, by Theorem 4.1, there exists a positive hermitian  $F$ -linear functional  $L$  on  $\mathfrak{F}$  such that

$$J = \{a \in \mathfrak{F} \mid L(a^*a) = 0\}.$$

By the GNS construction, there exists an  $\mathcal{R}$ -point  $(\pi, v)$  such that  $L(a) = \langle \pi(a)v, v \rangle$  for every  $a \in \mathfrak{F}$ . (Recall that  $V_\pi = \mathfrak{F}/J$  considered as a vector space over  $F$  with inner product  $\langle p + J, q + J \rangle = L(q^*p)$ ,  $\pi$  is the left regular representation of  $\mathfrak{F}$  on  $V_\pi$  and  $v = 1 + J$ .) It follows that

$$J = \mathcal{I}(\{(\pi, v)\}).$$

By the last claim of Lemma 1.4,

$$\sqrt[r]{J} = J.$$

Hence,  $\sqrt[r]{I} \subseteq J$ . By Lemma 1.5, also  $J \subseteq \sqrt[r]{I}$ . □

5. CHARACTERIZATIONS OF  $\sqrt[\mathcal{R}]{I}$  AND  $\sqrt[\mathcal{R}]{I}$  IN GENERAL  $*$ -ALGEBRAS

The main result of this section is Proposition 5.8 which gives an iterative procedure for computing  $\sqrt[\mathcal{R}]{I}$  in general  $*$ -algebras. We also discuss the relation of this result to the Real Algorithm.

**5.1. A Topological Characterization of  $\sqrt[\mathcal{R}]{I}$ .** Let  $\mathcal{A}$  be a  $*$ -algebra. Write  $\Sigma_{\mathcal{A}}$  for the set of all finite sums of elements  $a^*a$ ,  $a \in \mathcal{A}$ . We assume that  $\mathcal{A}_h$  is equipped with the finest locally convex topology, i.e., the finest vector space topology whose every neighborhood of zero contains a convex balanced absorbing set. Equivalently, it is the coarsest topology for which every seminorm on  $\mathcal{A}_h$  is continuous. In this case, every linear functional  $f$  on  $\mathcal{A}_h$  is continuous since  $|f|$  is a seminorm.

Suppose that  $C$  is a convex cone on  $\mathcal{A}_h$ . Write  $C^\vee$  for the set of all linear functionals  $f$  on  $\mathcal{A}_h$  such that  $f(C) \geq 0$  and write  $C^{\vee\vee}$  for the set of all  $v \in \mathcal{A}_h$  such that  $f(v) \geq 0$  for every  $f \in C^\vee$ . By the Separation Theorem for convex sets [1, II.39, Corollary 5],  $C^{\vee\vee} = \overline{C}$ . It follows that for every elements  $a, b \in \mathcal{A}_h$  such that  $a + \varepsilon b \in C$  for every real  $\varepsilon > 0$ , we have that  $a \in \overline{C}$ .

Note that every  $\Sigma_{\mathcal{A}}$ -positive linear functional  $f$  on the real vector space  $\mathcal{A}_h$  extends uniquely to a positive hermitian  $F$ -linear functional on the  $*$ -algebra  $\mathcal{A}$  (namely, take  $\tilde{f}(a) = \frac{1}{2}f(a+a^*)$  if  $F = \mathbb{R}$  and  $\tilde{f}(a) = \frac{1}{2}(f(a+a^*) - if(ia - ia^*))$  if  $F = \mathbb{C}$ ), hence by the GNS construction, see e.g. [11, Section 8.6], there exists a  $*$ -representation  $\pi$  of  $\mathcal{A}$  and  $v \in V_\pi$  such that  $f(a) = \langle \pi(a)v, v \rangle$  for every  $a \in \mathcal{A}_h$ .

**Theorem 5.1.** *Let  $I$  be a left ideal in  $*$ -algebra  $\mathcal{A}$  and let  $\Sigma_I$  be the set of all finite sums of elements  $u^*u$  where  $u \in I$ . Then*

$$\sqrt[\mathcal{R}]{I} = \{a \in \mathcal{A} \mid -a^*a \in \overline{\Sigma_{\mathcal{A}} - \Sigma_I}\}$$

*Proof.* Pick  $a \in \mathcal{A}$  and recall that  $a \in \sqrt[\mathcal{R}]{I}$  if and only if  $\pi(a)v = 0$  for every  $\mathcal{R}$ -point  $(\pi, v)$  such that  $\pi(x)v = 0$  for every  $x \in I$ . Clearly, the latter is true if and only if  $\langle \pi(-a^*a)v, v \rangle \geq 0$  for every  $\mathcal{R}$ -point  $(\pi, v)$  such that  $\langle \pi(-x^*x)v, v \rangle \geq 0$  for every  $x \in I$ . By the GNS construction, this is equivalent to  $f(-a^*a) \geq 0$  for every linear functional  $f$  on  $\mathcal{A}_h$  such that  $f(\Sigma_{\mathcal{A}}) \geq 0$  and  $f(-x^*x) \geq 0$  for every  $x \in I$  or, in other words, to  $-a^*a \in (\Sigma_{\mathcal{A}} - \Sigma_I)^{\vee\vee} = \overline{\Sigma_{\mathcal{A}} - \Sigma_I}$ .  $\square$

Further characterizations of  $\sqrt[\mathcal{R}]{I}$  can be obtained by combining Theorem 5.1 with Proposition 5.2.

**Proposition 5.2.** *Let  $\mathcal{A}$  be as above and let  $I$  be a left ideal of  $\mathcal{A}$  generated by the set  $\{p_\lambda\}_{\lambda \in \Lambda}$ . Write  $S$  for the set  $\{p_\lambda^*p_\lambda\}_{\lambda \in \Lambda}$ . Then*

$$\Sigma_{\mathcal{A}} - \text{cone}(S) \subseteq \Sigma_{\mathcal{A}} - \Sigma_I \subseteq \Sigma_{\mathcal{A}} + (I \cap \mathcal{A}_h) \subseteq (\Sigma_{\mathcal{A}} + I + I^*) \cap \mathcal{A}_h$$

and

$$\overline{\Sigma_{\mathcal{A}} - \text{cone}(S)} = \overline{\Sigma_{\mathcal{A}} - \Sigma_I} = \overline{\Sigma_{\mathcal{A}} + (I \cap \mathcal{A}_h)} = \overline{(\Sigma_{\mathcal{A}} + I + I^*) \cap \mathcal{A}_h}.$$

*Proof.* Clearly,  $\text{cone}(S) \subseteq \Sigma_I \subseteq I \cap \mathcal{A}_h \subseteq (I + I^*) \cap \mathcal{A}_h$ , which implies the claimed inclusions. To prove the equalities, it suffices to show that  $(\Sigma_{\mathcal{A}} + I + I^*) \cap \mathcal{A}_h \subseteq \overline{\Sigma_{\mathcal{A}} - \text{cone}(S)}$ . Take any  $x \in (\Sigma_{\mathcal{A}} + I + I^*) \cap \mathcal{A}_h$  and pick  $s \in \Sigma_{\mathcal{A}}$ ,  $u, v \in I$  such that  $x = s + u + v^*$ . It follows that

$$x = \frac{1}{2}(x + x^*) = s + \frac{1}{2}(u + v) + \frac{1}{2}(u + v)^* = s + w + w^*$$

where  $w = \frac{1}{2}(u + v) \in I$ . By the definition of generators, there exists a finite subset  $M$  of  $\Lambda$  and elements  $q_\mu \in \mathcal{A}$ ,  $\mu \in M$ , such that  $w = \sum_{\mu \in M} q_\mu p_\mu$ . For every  $\varepsilon > 0$ , we have that

$$\begin{aligned} x + \varepsilon \sum_{\mu \in M} q_\mu q_\mu^* &= s + \sum_{\mu \in M} q_\mu p_\mu + \sum_{\mu \in M} p_\mu^* q_\mu^* + \varepsilon \sum_{\mu \in M} q_\mu q_\mu^* \\ &= s + \frac{1}{\varepsilon} \sum_{\mu \in M} (p_\mu + \varepsilon q_\mu^*)^* (p_\mu + \varepsilon q_\mu^*) - \frac{1}{\varepsilon} \sum_{\mu \in M} p_\mu^* p_\mu \in \Sigma - \text{cone}(S). \end{aligned}$$

It follows that  $x \in \overline{\Sigma_{\mathcal{A}} - \text{cone}(S)}$ .  $\square$

Corollary 5.3 bears some resemblance to Theorem 7 in [4]. The closure in the finest locally convex topology, replaces the approximation and archimedean term appearing in that Theorem.

**Corollary 5.3.** *For every left ideal  $I$  of  $\mathcal{A}$*

$$\sqrt[\mathcal{R}]{I} = \{a \in \mathcal{A} \mid -a^*a \in \overline{(\Sigma_{\mathcal{A}} + I + I^*) \cap \mathcal{A}_h}\}.$$

Worth mentioning is also

**Corollary 5.4.** *Suppose that  $\{p_\lambda\}_{\lambda \in \Lambda}$  is a subset of  $\mathcal{A}$ . If  $a \in \mathcal{A}$  satisfies  $\pi(a)v = 0$  for every  $\mathcal{R}$ -point  $(\pi, v)$  of  $\mathcal{A}$  such that  $\pi(p_\lambda)v = 0$  for all  $\lambda \in \Lambda$ , then  $-a^*a \in \overline{\Sigma_{\mathcal{A}} - \text{cone}(S)}$  where  $S = \{p_\lambda^* p_\lambda\}_{\lambda \in \Lambda}$ .*

**5.2. An Auxiliary “Radical”  $\sqrt[\circ]{I}$ .** Corollary 5.3 suggests that for every left ideal  $I$  of a  $*$ -algebra  $\mathcal{A}$ , the following set is relevant:

$$\sqrt[\circ]{I} := \{a \in \mathcal{A} \mid -a^*a \in \Sigma_{\mathcal{A}} + I + I^*\}.$$

Note that  $\sqrt[\circ]{I} \subseteq \sqrt[\mathcal{R}]{I}$  by the definition of a real ideal.

The remainder of this section is devoted to a discussion of when  $\sqrt[\circ]{I}$  is an ideal. The next example shows that it need not be, even for a principal left ideal in a free  $*$ -algebra.

**Example 5.5.** Let  $I \subset \mathfrak{F} = F\langle x, x^* \rangle$  be the left ideal generated by the polynomial  $x_1^* x_1$ . Clearly,  $x_1 \in \sqrt[3]{I}$ . We claim that  $x_1^2 \notin \sqrt[3]{I}$ .

If  $x_1^2 \in \sqrt[3]{I}$ , then  $(x_1^2)^* x_1^2 + \sigma \in I + I^*$  for some  $\sigma \in \Sigma_{\mathfrak{F}}$ . By part (2) of Proposition 2.20, we get  $x_1^2 \in I \oplus \mathfrak{F}_1$ , which is not possible.  $\square$

If the set  $(\Sigma_{\mathcal{A}} + I + I^*) \cap \mathcal{A}_h$  is closed, then  $\sqrt[3]{I} = \sqrt[2]{I}$  by Corollary 5.3. It follows that the set  $\sqrt[3]{I}$  is a left ideal and  $\sqrt[3]{I} = \sqrt[2]{I}$ .

There exists a large class of  $*$ -algebras in which  $\sqrt[3]{I}$  is always a left ideal. We say that a  $*$ -algebra  $\mathcal{A}$  is *centrally bounded* if for every  $a \in \mathcal{A}$ , there exists an element  $c$  in the center of  $\mathcal{A}$  such that  $c^* c - a^* a \in \Sigma_{\mathcal{A}}$ .

**Lemma 5.6.** *If  $I$  is a left ideal of an centrally bounded  $*$ -algebra  $\mathcal{A}$  then the set  $\sqrt[3]{I}$  is also a left ideal of  $\mathcal{A}$ .*

*Proof.* Suppose that  $a, b \in \sqrt[3]{I}$ . Hence,  $-a^* a, -b^* b \in \Sigma_{\mathcal{A}} + I + I^*$  by the definition of  $\sqrt[3]{I}$ . It follows that

$$-(a+b)^*(a+b) = (a-b)^*(a-b) + 2(-a^*a) + 2(-b^*b) \in \Sigma_{\mathcal{A}} + I + I^*.$$

Therefore,  $a+b \in \sqrt[3]{I}$ . Suppose now that  $a \in \mathcal{A}$  and  $b \in \sqrt[3]{I}$ . Since  $\mathcal{A}$  is centrally bounded, there exists  $c$  in the center of  $\mathcal{A}$  such that  $c^* c - a^* a \in \Sigma_{\mathcal{A}}$ . Since  $-b^* b \in \Sigma_{\mathcal{A}} + I + I^*$ , it follows that

$$-b^* a^* a b = c^* c (-b^* b) + b^* (c^* c - a^* a) b \in \Sigma_{\mathcal{A}} + I + I^*.$$

Therefore  $ab \in \sqrt[3]{I}$ .  $\square$

Clearly, every commutative unital algebra is centrally bounded as well as every algebraically bounded  $*$ -algebra (in particular, every Banach  $*$ -algebra and every group algebra with standard involution  $g^* = g^{-1}$ ). We would like to show that algebras of matrix polynomials are also centrally bounded. This follows from the following observation.

**Lemma 5.7.** *If  $\mathcal{A}$  is a centrally bounded  $*$ -algebra, then  $M_n(\mathcal{A})$  is also a centrally bounded  $*$ -algebra for every  $n$ .*

*Proof.* Every element  $P \in M_n(\mathcal{A})$  can be written as  $P = \sum_{i,j=1}^n p_{ij} E_{ij}$  where  $E_{ij}$  are matrix units. Since  $I - E_{ij}^* E_{ij} = I - E_{jj} = \sum_{i \neq j} E_{ii} = \sum_{i \neq j} E_{ii}^* E_{ii}$ , all matrix units are centrally bounded. By assumption, elements  $p_{ij} I$  are also centrally bounded. Therefore it suffices to show that a sum and a product of two centrally bounded elements is a centrally bounded element. Suppose that  $c_i^* c_i - P_i^* P_i \in \Sigma_{\mathcal{A}}$  for  $i = 1, 2$  where  $c_i$  are central and  $P_i$  are arbitrary elements of  $\mathcal{A}$ . It follows that

$$\begin{aligned} & (1 + c_1^* c_1 + c_2^* c_2)^2 - (P_1 + P_2)^*(P_1 + P_2) = \\ & = 1 + (c_1^* c_1 + c_2^* c_2)^2 + 2 \sum_{i=1}^2 (c_i^* c_i - P_i^* P_i) + (P_1 - P_2)^*(P_1 - P_2) \in \Sigma_{\mathcal{A}} \end{aligned}$$

and

$$\begin{aligned} & (c_1 c_2)^*(c_1 c_2) - (P_1 P_2)^*(P_1 P_2) = \\ & = P_2^*(c_1^* c_1 - P_1^* P_1) P_2 + c_1^*(c_2^* c_2 - P_2^* P_2) c_1 \in \Sigma_{\mathcal{A}}. \end{aligned}$$

□

**5.3. An Iterative Description of  $\sqrt[r]{I}$ .** For a left ideal  $I$  in a  $*$ -algebra  $\mathcal{A}$ , let  $\sqrt[\beta]{I}$  denote the left ideal in  $\mathcal{A}$  generated by  $\sqrt[\alpha]{I}$ ; i.e.

$$\sqrt[\beta]{I} := \mathcal{A} \sqrt[\alpha]{I}.$$

Unlike the real radical,  $\sqrt[\beta]{\cdot}$  is not idempotent. However, we do have the following:

**Proposition 5.8.** *If  $I$  is a left ideal of a  $*$ -algebra  $\mathcal{A}$ , then*

$$\sqrt[\beta]{I} \cup \sqrt[\beta]{\sqrt[\beta]{I}} \cup \sqrt[\beta]{\sqrt[\beta]{\sqrt[\beta]{I}}} \cup \dots = \sqrt[r]{I}.$$

*Proof.* Write  $I_0 = I$  and  $I_{n+1} = \sqrt[\beta]{I_n}$  for every  $n = 0, 1, 2, \dots$ . Hence, the left-hand side of the formula is  $J := \bigcup_{n=0}^{\infty} I_n$ . To show that  $J \subseteq \sqrt[r]{I}$ , it suffices to show that  $I_n \subseteq \sqrt[r]{I}$  for every  $n$ . This is clear for  $n = 0$ . Suppose this is true for some  $n$  and pick  $x \in I_{n+1}$ . By the definition of  $I_{n+1}$ ,  $x = \sum_{i=1}^k a_i y_i$ , where  $a_i \in \mathcal{A}$  and  $-y_i^* y_i \in \Sigma_{\mathcal{A}} + I_n + I_n^*$  for  $i = 1, \dots, k$ . Since  $I_n \subseteq \sqrt[r]{I}$  and  $\sqrt[r]{I}$  is real, it follows that  $y_i \in \sqrt[r]{I}$  for every  $i = 1, \dots, k$ . Hence  $x \in \sqrt[r]{I}$ . We will prove the opposite inclusion  $\sqrt[r]{I} \subseteq J$  by showing that  $J$  is real. Pick  $u_1, \dots, u_r \in \mathcal{A}$  such that  $\sum_{i=1}^r u_i^* u_i \in J + J^*$ . By the definition of  $J$ , there exists a number  $n$  and elements  $b, c \in I_n$  such that  $\sum_{i=1}^r u_i^* u_i = b + c^*$ . It follows that for every  $i = 1, \dots, r$ ,  $-u_i^* u_i \in \Sigma_{\mathcal{A}} + I_n + I_n^*$ . Therefore  $u_i \in \sqrt[\beta]{I_n} \subseteq \sqrt[\beta]{I_n} = I_{n+1} \subseteq J$ . □

Specializing the iterative procedure of Proposition 5.8, which works in all  $*$ -algebras, to the case of a left ideal in free  $*$ -algebra does not lead to the Real Algorithm. Here is an informal comparison:

- (1) Proposition 5.8 adds all tuples  $(q_i)$  such that  $\sum_i q_i^* q_i \in I_k + I_k^*$  to  $I_k$  to produce the update  $I_{k+1}$ ; whereas the Real Algorithm adds one such tuple  $(q_i)$  which was well chosen to  $I^{(k)}$  to produce  $I^{(k+1)}$ .
- (2) For a general  $*$ -algebra  $\mathcal{A}$  and left ideal  $I$ , the iterations in Proposition 5.8 do not necessarily stop unless  $\mathcal{A}$  is left noetherian (such as  $M_n(F[x])$ , see §6.) However, in the case  $I$  is a left ideal in the free  $*$ -algebra  $\mathfrak{F}$ , the inclusion sense for finitely generated left ideals in  $I^{(k)} \subseteq I_k$  implies the procedure of Proposition 5.8 does terminate.

- (3) Unlike the Real Algorithm, even if only finitely many iterations are needed in Proposition 5.8, it does not tell us how to obtain generators of  $\sqrt[r]{I}$  from the generators of  $I$ . (This is a nontrivial problem even for  $\mathbb{R}[x]$ , cf. [6] for a partial solution, and it is still open for  $M_n(F[x])$ .)

For centrally bounded algebras, Proposition 5.8 and Lemma 5.6 imply the following simple iterative description of the elements of the real radical:

**Corollary 5.9.** *Let  $I$  be a left ideal of a centrally bounded  $*$ -algebra  $\mathcal{A}$ . An element  $x \in \mathcal{A}$  belongs to  $\sqrt[r]{I}$  if there exist  $m \in \mathbb{N}$ ,  $s_1, \dots, s_m \in \Sigma_{\mathcal{A}}$  and  $k_1, \dots, k_m \in \{a \in \mathcal{A} \mid a^* = -a\}$  such that the last term of the sequence*

$$x_1 := x, \quad x_{i+1} := x_i^* x_i + s_i + k_i, i = 1, \dots, m,$$

*belongs to  $I$ .*

For commutative  $*$ -algebras, we have the following classical real Nullstellensatz:

**Corollary 5.10.** *For every ideal  $I$  of a commutative  $*$ -algebra  $\mathcal{A}$  we have that*

$$\begin{aligned} \sqrt[r]{I} &= \{a \in \mathcal{A} \mid -(a^*a)^k \in \Sigma_{\mathcal{A}} + I + I^* \text{ for some } k\} \\ &= \{a \in \mathcal{A} \mid -(a^*a)^k \in \Sigma_{\mathcal{A}} + I \text{ for some } k\}. \end{aligned}$$

*Proof.* For every ideal  $J$  of  $\mathcal{A}$  write

$$\sqrt[r]{J} := \{a \in \mathcal{A} \mid -a^*a \in \Sigma_{\mathcal{A}} + J\}.$$

Since  $J \subseteq \sqrt[r]{J}$ ,  $(\sqrt[r]{J})^* = \sqrt[r]{J}$  and  $\sqrt[r]{J + J^*} = \sqrt[r]{J}$ , we have that

$$(5.1) \quad \sqrt[r]{J} \subseteq \sqrt[r]{J} \subseteq \sqrt[r]{\sqrt[r]{J}}.$$

If  $a \in \sqrt[r]{\sqrt[r]{J}}$  for some  $a \in \mathcal{A}$ , then  $a^*a + \sigma \in \sqrt[r]{J}$  for some  $\sigma \in \Sigma_{\mathcal{A}}$ . It follows that  $(a^*a + \sigma)^2 + \tau \in J$  for some  $\tau \in \Sigma_{\mathcal{A}}$ . Since  $2\sigma a^*a + \sigma^2 + \tau \in \Sigma_{\mathcal{A}}$ , it follows that  $a^*a \in \sqrt[r]{J}$ . Therefore

$$(5.2) \quad \sqrt[r]{\sqrt[r]{J}} = \{a \in \mathcal{A} \mid a^*a \in \sqrt[r]{J}\}.$$

For every ideal  $I$  of  $\mathcal{A}$  we define two sequences:

$$I_0 = I, I_{n+1} = \sqrt[r]{I_n} \quad \text{and} \quad K_0 = I, K_{n+1} = \sqrt[r]{K_n}.$$

By induction on  $n$ , using (5.1), we show that  $K_n \subseteq I_n \subseteq K_{2^n}$ . By Proposition 5.8, it follows that

$$(5.3) \quad \bigcup_{n=0}^{\infty} K_n = \bigcup_{n=0}^{\infty} I_n = \sqrt[r]{I}.$$

Note also that  $\sqrt[r]{I} = \sqrt[r]{I + I^*}$ , hence

$$\sqrt[r]{I} = \sqrt[r]{I + I^*}$$

by Proposition 5.8. On the other hand, equation (5.2) implies that

$$(5.4) \quad K_n = \{a \in \mathcal{A} \mid -(a^*a)^{2^{n-1}} \in \Sigma_{\mathcal{A}} + I\}.$$

To finish the proof, note that  $-(a^*a)^n \in \Sigma_{\mathcal{A}} + I$  implies  $-(a^*a)^{2^{n-1}} \in \Sigma_{\mathcal{A}} + I$ .  $\square$

## 6. A NULLSTELLENSATZ FOR $M_n(F[x])$

We will discuss the following question:

**Question:** Which left ideals  $I$  in  $M_n(F[x])$  satisfy  $\sqrt[\varepsilon]{I} = \sqrt[r]{I}$ ?

Recall that  $\sqrt[\varepsilon]{I} = \{Q \in M_n(F[x]) \mid Q(a)v = 0 \text{ for every } a \in \mathbb{R}^g \text{ and } v \in F^n \text{ such that } P(a)v = 0 \text{ for all } P(x) \in I\}$ .

We will prove the answer is yes for all  $I$  in the cases of  $g = 0$  and  $g = 1$  variables, see Propositions 6.2 and 6.3. The case of several variables remains undecided, except for  $n = 1$  which is classical, see Example 6.1

Example 6.1 rephrases the classical Real Nullstellensatz of Dubois [2], Risler [9] and Efroymson [3], and extends it from  $\mathbb{R}[x]$  to  $\mathbb{C}[x]$ .

**Example 6.1.** For every ideal  $I$  of  $F[x]$  we have that

$$\sqrt[\varepsilon]{I} = \sqrt[r]{I}.$$

If a polynomial  $q \in F[x]$  belongs to  $\sqrt[\varepsilon]{I}$ , then  $q(a)v = 0$  for every  $(a, v) \in \mathbb{R}^g \times F$  such that  $p(a)v = 0$  for all  $p \in I$ . It follows that  $q(a) = 0$  for every  $a \in \mathbb{R}^g$  such that  $p(a) = 0$  for all  $p \in I$ , hence  $(\bar{q}q)(a) = 0$  for every  $a \in \mathbb{R}^g$  such that  $(\bar{p}p)(a) = 0$  for all  $p \in I$ . By the classical Real Nullstellensatz, there exists  $k \in \mathbb{N}$  such that  $-(\bar{q}q)^{2k} \in \Sigma_{\mathcal{A}} + \text{ideal generated by } \bar{p}p, p \in I$ . It follows that  $q \in \sqrt[r]{I}$ .  $\square$

**Proposition 6.2.** For every left ideal  $I$  of  $M_n(F)$ , we have that

$$I = \sqrt[r]{I} = \sqrt[\varepsilon]{I}.$$



*Proof.* It suffices to show that  $\sqrt[n]{I} \subseteq I$ . Since  $M_n(F)$  is finite-dimensional,  $I$  is finitely generated, let  $B_1, \dots, B_r$  be the generators of  $I$  as a left ideal. It follows that

$$\sqrt[n]{I} = \{C \in M_n(F) \mid \ker \mathbf{B} \subseteq \ker C\} \quad \text{where} \quad \mathbf{B} = \begin{bmatrix} B_1 \\ \vdots \\ B_r \end{bmatrix}.$$

For each  $C \in \sqrt[n]{I}$ , one sees that  $\ker \mathbf{B} \subseteq \ker C$ , which implies that the row space of  $C$  is contained in the row space of  $\mathbf{B}$ . Therefore, there exists a matrix  $R = [R_1 \dots R_r]$  such that  $C = R\mathbf{B}$ . It follows that  $C \in I$ .  $\square$

**Theorem 6.3.** *For every positive integer  $n$  and every left ideal  $I$  in  $M_n(F[x_1])$  we have that*

$$\sqrt[n]{I} = \sqrt[r]{I}.$$

*Proof.* The proof consists of three steps:

- (1) Reduction to the case  $I = (P)$ , that is, the case where  $I$  is a principal ideal.
- (2) Reduction to the case where  $P$  is diagonal.
- (3) Induction on  $n$ .

Steps (1) and (3) also work for several variables but step (2) does not.

Since  $F[x_1]$  is left noetherian so is  $M_n(F[x_1])$ , see Proposition 1.2. in [8]. Therefore  $I = (P_1, \dots, P_k)$  for some  $P_1, \dots, P_k \in M_n(F[x_1])$ . Define  $P = P_1^*P_1 + \dots + P_k^*P_k$  and note that  $(P) \subseteq I \subseteq \sqrt[r]{(P)}$ . It follows that  $\sqrt[r]{I} = \sqrt[r]{(P)}$  and  $\sqrt[n]{I} = \sqrt[n]{(P)}$ , proving (1).

Let  $P = UDV$  be the Smith normal form of  $P$ , i.e.  $U$  and  $V$  are invertible in  $M_n(F[x_1])$  and  $D$  is diagonal. Since  $(P) = (DV)$ , it suffices to prove that  $\sqrt[n]{(DV)} = \sqrt[n]{(D)}V$  and  $\sqrt[r]{(DV)} = \sqrt[r]{(D)}V$ . Clearly,  $R \in \sqrt[n]{(DV)}$  iff  $R(a)w = 0$  for every  $a \in \mathbb{R}$  and  $w \in F^n$  such that  $D(a)V(a)w = 0$  iff  $R(a)V(a)^{-1}z = 0$  for every  $a \in \mathbb{R}$  and  $z \in F^n$  such that  $D(a)z = 0$  iff  $RV^{-1} \in \sqrt[n]{(D)}$ . To prove the second equality, it suffices to show that  $\sqrt[r]{(DV)} \subseteq \sqrt[r]{(D)}V$ . Namely, replacing  $V$  by  $V^{-1}$  and  $D$  by  $DV$ , we get the opposite inclusion. We have to show that the left ideal  $\sqrt[r]{(D)}V$ , which contains  $(DV)$ , is real. Suppose that  $\sum_i Q_i^*Q_i \in \sqrt[r]{(D)}V$  for some  $Q_i$ . It follows that  $\sum_i (V^{-1})^*Q_i^*Q_iV^{-1} \in (V^{-1})^*\sqrt[r]{(D)} \subseteq \sqrt[r]{(D)}$ , hence  $Q_iV^{-1} \in \sqrt[r]{(D)}$  for all  $i$ .

We will show now that  $\sqrt[n]{(D)} = \sqrt[r]{(D)}$  by induction on  $n$ . For  $n = 1$  this is Example 6.1. Now we assume that  $\sqrt[n]{(D_1)} \subseteq \sqrt[r]{(D_1)}$  and  $\sqrt[n]{(D_2)} \subseteq \sqrt[r]{(D_2)}$  and claim that  $\sqrt[n]{(D_1 \oplus D_2)} \subseteq \sqrt[r]{(D_1 \oplus D_2)}$ .

Pick any  $R = [R_1 \ R_2] \in \sqrt[\varepsilon]{(D_1 \oplus D_2)}$ . From the definition of  $\sqrt[\varepsilon]{\phantom{x}}$  we get that  $R_1(a)v_1 + R_2(a)v_2 = 0$  for every  $a \in \mathbb{R}$ ,  $v_1 \in F^{n_1}$  and  $v_2 \in F^{n_2}$  such that  $D_1(a)v_1 = 0$  and  $D_2(a)v_2 = 0$ . Inserting either  $v_2 = 0$  or  $v_1 = 0$  we get (for each  $i$ ) that  $R_i(a)v_i = 0$  for every  $a \in \mathbb{R}$  and  $v_i \in F^{n_i}$  such that  $D_i(a)v_i = 0$ . Note that  $R_i(a)v_i = 0$  implies  $R_i(a)^*R_i(a)v_i = 0$  and that  $R_i^*R_i$  is a square matrix of size  $n_i$ . It follows that  $R_i^*R_i \in \sqrt[\varepsilon]{(D_i)} \subseteq \sqrt[\text{r}]{(D_i)}$ . Let  $j_i: M_{n_i}(F[x_1]) \rightarrow M_{n_1+n_2}(F[x_1])$  be the natural embeddings. Since  $j_i$  are  $*$ -homomorphisms and  $J_i = \sqrt[\text{r}]{(j_i(D_i))}$  are real left ideals,  $j_i^{-1}(J_i)$  are also real left ideals, so that  $\sqrt[\text{r}]{(D_i)} \subseteq j_i^{-1}(J_i)$ . Since  $j_i(D_i)$  is the product of  $j_i(I_{n_i})$  and  $D_1 \oplus D_2$ , it belongs to  $(D_1 \oplus D_2)$ . Hence, for  $i = 1, 2$ ,

$$j_i(R_i^*R_i) \in j_i(\sqrt[\text{r}]{(D_i)}) \subseteq \sqrt[\text{r}]{(j_i(D_i))} \subseteq \sqrt[\text{r}]{(D_1 \oplus D_2)}.$$

Since  $[R_1 \ 0]^* [R_1 \ 0] = j_1(R_1^*R_1)$  and  $[0 \ R_2]^* [0 \ R_2] = j_2(R_2^*R_2)$  belong to  $\sqrt[\text{r}]{(D_1 \oplus D_2)}$ ,  $[R_1 \ 0]$  and  $[0 \ R_2]$  also belong to  $\sqrt[\text{r}]{(D_1 \oplus D_2)}$ . Therefore,  $[R_1 \ R_2] = [R_1 \ 0] + [0 \ R_2] \in \sqrt[\text{r}]{(D_1 \oplus D_2)}$ .  $\square$

## REFERENCES

- [1] N. Bourbaki, *Topological vector spaces, Chapters 1-5*, English edition, Springer Verlag, Masson 1987.
- [2] D. W. Dubois, A nullstellensatz for ordered fields, *Ark. Mat.* 8 (1969), 111–114.
- [3] G. Efroymson, Local reality on algebraic varieties, *J. Algebra* 29 (1974), 113–142.
- [4] J. W. Helton, S. McCullough, M. Putinar, Strong majorization in a free  $*$ -algebra, *Math. Z.* 255 (2007), no. 3, 579–596.
- [5] T. Y. Lam, An introduction to real algebra, *Rocky Mountain J. Math.* 14 (1984), no. 4, 767–814.
- [6] J. B. Lasserre, M. Laurent, P. Rostalski, Semidefinite characterization and computation of zero-dimensional real radical ideals, *Found. Comput. Math.* 8 (2008), no. 5, 607–647.
- [7] M. Marshall,  $*$ -orderings on a ring with involution, *Comm. Algebra* 28 (2000), no. 3, 1157–1173.
- [8] J. C. McConnell, J. C. Robson, Noncommutative Noetherian rings. With the cooperation of L. W. Small. Revised edition. Graduate Studies in Mathematics, 30. American Mathematical Society, Providence, RI, 2001. xx+636 pp. ISBN: 0-8218-2169-5.
- [9] J.-J. Risler, Une caractérisation des idéaux des variétés algébriques réelles. *C.R.A.S. Paris, série A*, 271 (1970), 1171–1173.
- [10] S. Shankar, The Nullstellensatz for Systems of PDE, *Advances in Applied Mathematics* 23 (1999), 360–374.
- [11] K. Schmüdgen, *Unbounded Operator Algebras and Representation Theory*, Birkhäuser Verlag, Basel 1990.

- [12] K. Schmüdgen, Noncommutative real algebraic geometry - some basic concepts and first ideas. Emerging applications of algebraic geometry, 325-350, IMA Vol. Math. Appl., 149, Springer, New York, 2009.

JAKOB CIMPRIČ, DEPARTMENT OF MATHEMATICS, UNIVERSITY OF LJUBLJANA, JADRANSKA 21, SI-1000 LJUBLJANA, SLOVENIA

*E-mail address:* cimpric@fmf.uni-lj.si

*URL:* <http://www.fmf.uni-lj.si/~cimpric/>

J. WILLIAM HELTON, DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CALIFORNIA SAN DIEGO, 9500 GILMAN DRIVE, LA JOLLA, CALIFORNIA 92093-0112, USA

*E-mail address:* helton@math.ucsd.edu

*URL:* <http://math.ucsd.edu/~helton/>

SCOTT MCCULLOUGH, DEPARTMENT OF MATHEMATICS, UNIVERSITY OF FLORIDA, 490 LITTLE HALL, GAINESVILLE, FLORIDA 32611-8105, USA

*E-mail address:* sam@math.ufl.edu

*URL:* <http://www.math.ufl.edu/~sam/>

CHRISTOPHER NELSON, DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CALIFORNIA SAN DIEGO, 9500 GILMAN DRIVE, LA JOLLA, CALIFORNIA 92093-0112, USA

*E-mail address:* csnelson@math.ucsd.edu